LECTURES ON THE AFL FOR GL_2

ANDREAS MIHATSCH

Contents

The aim of this course is to understand the proof and context of the so-called Arithmetic Fundamental Lemma (AFL) for GL_2.

Theorem 0.1 (AFL for GL_2)**.** *Let $\gamma \in GL_2(\mathbb{Q}_p)$ be a regular semi-simple and matches to an element $g \in B^\times$ in the quaternion division algebra over $\mathbb{Q}_p$. Then there is an identity*

$$\left.\frac{d}{ds}\right|_{s=0} O(\gamma, 1_{GL_2(\mathbb{Z}_p)}, s) = \pm \mathrm{Int}(g) \log(p). \tag{0.1}$$

The left hand side is the first derivative of an orbital integral that is related to the derivative of an L-function. The right hand side is an intersection number on Lubin–Tate space that is related to heights of points on elliptic curves. We will see precise definitions of all occurring terms during the course.

My plan is as follows. In the first lecture, I will motivate the intersection-theoretic side of (0.1). We will then spend several lectures to work out everything in detail. Having achieved this, we will look at a relative trace formula comparison that defines the analytic side in (0.1) and proof Thm. 0.1.

1. Intersecting Heegner Divisors

1.1. **Ranks of elliptic curves.** Recall that an elliptic curve is a proper, smooth, connected group scheme of dimension 1. They are always commutative and of genus 1.

Theorem 1.1 (Mordell–Weil)**.** *For every number field $K/\mathbb{Q}$ and every elliptic curve E/K, the group of rational points $E(K)$ is finitely generated.*

Date: June 27, 2022.

Compare this with the situation for curves of other genus. If C/K is a proper smooth curve of genus 0, then C is a Galois twist of $\mathbb{P}^1_K$. More precisely, if $C(K) \neq \emptyset$, then one may pick any point $x \in C(K)$ and use the degree 1 line bundle $\mathcal{O}_C(x)$ to define an isomorphism $C \cong \mathbb{P}^1_K$. If $C(K) = \emptyset$, then it is known that $C(K') \neq \emptyset$ for a suitable quadratic extension K'/K and hence $C_{K'} \cong \mathbb{P}^1_{K'}$.

If the genus of C/K is ≥ 2 on the other hand, then $C(K)$ is finite (Mordell Conjecture, Faltings 1986 [3]). In this sense, elliptic curves lie just between the trivial and the general situation, and much interest lies with the structure of $E(K)$, especially its rank.

Example 1.2. (1) The elliptic curve defined in $\mathbb{P}^2_{\mathbb{Q}}$ by

$$E : y^2 + y = x^3 - x^2$$

has $E(\mathbb{Q}) \cong \mathbb{Z}/5$. Its conductor is 11, the smallest possible, see here.

(2) The elliptic curve defined in $\mathbb{P}^2_{\mathbb{Q}}$ by

$$E : y^2 + y = x^3 + x^2$$

has $E(\mathbb{Q}) \cong \mathbb{Z}$ with generator $(0, 0)$. Its conductor is 43, see here.

Fix some number field K and consider all elliptic curves E/K. It is currently unknown whether the set of possible ranks $\mathrm{rk}_{\mathbb{Z}} E(K)$ is bounded or not. The current rank record for $K = \mathbb{Q}$ is an example of a curve with rank ≥ 28; it is due to Elkies (2006), see here. There are statistical results, however, for example 50% of elliptic curves over $\mathbb{Q}$ have $\mathrm{rk}_{\mathbb{Z}} E(\mathbb{Q}) = 0$.

The torsion in $E(K)$ is known to be bounded in terms of $[K : \mathbb{Q}]$ however.

Theorem 1.3 (Mazur's Theorem [6], Merel [7])**.** *(1) Let $d \geq 1$ be an integer. Then there exists an explicit bound $c \geq 0$ such that for every number field $K/\mathbb{Q}$ of degree $\leq d$ and every elliptic curve E/K,*

$$|E(K)_{\mathrm{tors}}| \leq c.$$

(2) Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})_{\mathrm{tors}}$ is one of the following 15 possibilities.

$$\mathbb{Z}/n, \quad 1 \leq n \leq 10 \text{ or } n = 12, \quad \mathbb{Z}/2 \times \mathbb{Z}/2m, \quad 1 \leq m \leq 4.$$

Given a point $x \in E(K)$, this in particular provides an algorithm for checking whether x is torsion or not. Namely one is only required to check all multiples $2x$, $3x, \ldots$ up to the bound provided by Thm. 1.3.

Coming back to the question for $\mathrm{rk}_{\mathbb{Z}} E(K)$, Birch and Swinnerton-Dyer conjectured a relation with the L-function $L(E/K, s)$ of E. Loosely speaking, the L-function packages the information of all the reductions $E_{\mathfrak{p}}$ of E modulo $\mathfrak{p} \in \operatorname{Spec} O_K$ (after choosing some integral model) and the conjecture can be understood as saying that $\mathrm{rk}_{\mathbb{Z}} E(K)$ is determined by the sizes of all $E_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$.

Conjecture 1.4. There is an equality

$$\mathrm{rk}_{\mathbb{Z}} E(K) = \mathrm{ord}_{s=1} L(E/K, s).$$

The conjecture is generally open (and one of the seven Millennium Prize problems). By work of Gross–Zagier [5] (1986), Kolyvagin (1991) and the Modularity Theorem of Wiles (1995) and Breuil–Conrad–Diamond–Taylor (2001), it is known for $E/\mathbb{Q}$ that

$$\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = 0 \text{ resp. } 1 \quad \Rightarrow \quad \mathrm{rk}_{\mathbb{Z}} E(\mathbb{Q}) = 0 \text{ resp. } 1.$$

1.2. **Heegner Points.** We work over $\mathbb{Q}$ from now on. The previous discussion leads one to ask for methods to construct rational points on elliptic curves. A general method is due to Heegner (1952) and relies on the modular curve.

Let $Y_0(N)$ be the open modular curve over $\mathbb{Q}$ of level $\Gamma_0(N)$. It is an affine smooth curve that may be described as the coarse moduli space of elliptic curves A together with a cyclic subgroup $C \subseteq A$ of order N. Denote by $X_0(N)$ its smooth compactification.

By the Modularity Theorem[1] every $E/\mathbb{Q}$ admits a non-constant map

$$f : X_0(N) \to E.$$

Such a map f is called a *modular parametrization* of E, the smallest possible N for which such an f exists is the *conductor* of E, compare Ex. 1.2.

There are two distinguished points $0, \infty \in (X_0(N) \setminus Y_0(N))(\mathbb{Q})$ corresponding to the "degenerate elliptic curves" $0 = (\mathbb{G}_m, \mu_N)$ and $\infty = (\mathbb{Z}/N \times \mathbb{G}_m, \mathbb{Z}/N)$. The modular parametrization is chosen such that $f(0) = 0$ in E.

Our aim (and Heegner's idea) is to construct specific points on $X_0(N)$ and then apply f to get points on E. Let $K/\mathbb{Q}$ be an imaginary quadratic field and fix an embedding $\tau : K \to \mathbb{C}$. Consider pairs (A, ι), where $A/\mathbb{C}$ is an elliptic curve and $\iota : O_K \to \mathrm{End}(A)$ an action of O_K such that the induced action

$$O_K \to \mathrm{End}(A) \to \mathrm{End}(\mathrm{Lie}\, A) = \mathbb{C}$$

is just τ itself.

Proposition 1.5. *The isomorphism classes of such pairs (A, ι) are in bijection with the class group Cl_K by*

$$\begin{aligned} \{(A,\iota)\}/\cong &\longrightarrow Cl_K \\ (\mathbb{C}/\Lambda, \iota) &\longmapsto [\Lambda] \text{ as } O_K\text{-module} \\ (\mathbb{C}/\tau(\mathcal{I}), \tau) &\longleftarrow\!\shortmid [\mathcal{I}]. \end{aligned} \tag{1.1}$$

We leave the proof as an exercise. At some point, we saw the following argument in class: Given $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$ and an elliptic curve $A/\mathbb{C}$,

$$j(\mathrm{Spec}\,\mathbb{C} \times_{\mathrm{Spec}\,\sigma, \mathrm{Spec}\,\mathbb{C}} A) = \sigma(j(A)).$$

This is just because j is a polynomial in the coefficients of some Weierstraß equation for A and the base change elliptic curve is defined by applying σ to these coefficients. Since the set (1.1) is finite, this implies that every A with CM by O_K is defined over a number field. In fact, one can show that each pair (A, ι) is defined over the Hilbert class field H_K/K of K and that $\mathrm{Gal}(H_K/K)$ acts simply transitive on (1.1).

Since we want to define points on $X_0(N)$, we now assume that every $p \mid N$ splits in O_K. Then (check this!) there is an ideal $\mathcal{N} \subseteq O_K$ such that $O_K/\mathcal{N} \cong \mathbb{Z}/N$ is cyclic. Thus we may define a map

$$\begin{aligned} Cl_K &\longrightarrow X_0(N)(H_K) \\ [\mathcal{I}] &\longmapsto x_{[\mathcal{I}]} := \left(\mathbb{C}/\tau(\mathcal{I}), \tau(\mathcal{N}^{-1}\mathcal{I})/\tau(\mathcal{I})\right). \end{aligned} \tag{1.2}$$

These are the famous Heegner points and our interest lies with their images $f(x_{[\mathcal{I}]}) \in E(H_K)$. Taking their sum, we find a K-rational point

$$x_K := \sum_{[\mathcal{I}] \in Cl_K} f(x_{[\mathcal{I}]}) \in E(K)$$

[1]This was not known at the time of Heegner or Gross–Zagier, of course. They did their work under the assumption that such a map exists.

and the fundamental question is whether or not x_K is torsion. Gross–Zagier [5] solved this problem in the style of the BSD Conjecture. Namely they define a certain L-function $L(E,\chi,s)$ and show:

Theorem 1.6 (Gross–Zagier)**.** *The point x_K is non-torsion if and only if $L'(E,\chi,1)\neq 0$.*

They actually prove the precise formula

$$L'(E,\chi,1)=\frac{8\pi^2(f,f)}{hu^2|D|^{1/2}}\widehat{h}(x_K) \tag{1.3}$$

where $u=|O_K^\times|$, where D is the discriminant of $K/\mathbb{Q}$, where h denotes the class number of K, and where (f,f) is the Petersson inner product of the modular form corresponding to E. The term $\hat{h}(x_K)$ is the canonical height of x_K and figures prominently in the next section.

1.3. **Intersection Theory.** Let us from now on work with a concrete example, namely the elliptic curve of conductor 43 from Example 1.2. This is in fact the only curve over $\mathbb{Q}$ of that conductor, so $E=X_0(43)$. The origin of E is $\infty=(\mathbb{G}_m,\mu_{43})$ as before. Given an imaginary quadratic field K such that 43 splits in K, we have constructed a point $x_K\in E(K)$.

Now recall that there is a height pairing (canonical height) on elliptic curves,

$$(\ ,\ ):E(\overline{\mathbb{Q}})\times E(\overline{\mathbb{Q}})\to\mathbb{R}_{>0}.$$

It is bilinear, symmetric and positive definite in the sense that

$$(x,x)>0\quad\Leftrightarrow\quad x\notin E(\overline{\mathbb{Q}})_{\mathrm{tors}}.$$

In particular, x_K is non-torsion if and only if

$$\widehat{h}(x_K):=(x_K,x_K)>0. \tag{1.4}$$

The above height pairing is closely related to intersection theory! More precisely, let

$$C=\sum m_i[c_i],\quad D=\sum m_j[d_j],\quad c_i,d_j\in E(K)$$

be divisors on E of degree 0 and such that $\operatorname{Supp}C\cap\operatorname{Supp}D=\emptyset$. Then

$$\Big(\sum m_ic_i,\sum m_jd_j\Big)=\sum_{v\in\Sigma_K}(C,D)_v$$

can be canonically decomposed into a sum of local height pairings. Here, Σ_K denotes the set of places of K and $(C,D)_v$ a certain pairing of degree 0 divisors on the local curve E_{K_v}. The interested reader is referred to the article [11, Chapter XIV] of Gross.

We now look at places $v\nmid 43,\infty$. (The archimedean places and the places above 43 are also interesting, of course, but this would be a separate discussion.) The curve $X_0(43)$ has a natural proper, smooth integral model over $\mathbb{Z}[1/43]$ which we denote by $\bar{E}$, namely the compactification of the coarse moduli space of elliptic curves with subgroup of order 43. Let $\bar{C},\bar{D}$ denote the closures of C and D in $O_K\otimes_{\mathbb{Z}}\bar{E}$. Then

$$(C,D)_v=(\bar{C},\bar{D})_{O_{K_v}\otimes_{\mathbb{Z}}\bar{E}}:=\ell_{O_{K,v}}(\mathcal{O}_{\bar{C}\cap\bar{D},v})\cdot\log(q_v)$$

is given by the intersection number of $\bar{C}$ and $\bar{D}$ on $O_{K_v}\otimes\bar{E}$. There is no self-intersection in the current situation, so this is just the length of the artinian O_{K_v}-module $\mathcal{O}_{\bar{C}\cap\bar{D},v}$.

In order to apply this to (x_K,x_K) from (1.4), we have to work with degree 0-divisors and circumvent the issue of self-intersection. For the former, we simply rewrite (1.4) as

$$\widehat{h}(x_K)=(x_K-0,x_K-\infty),$$

where $0, \infty \in X_0(43)(\mathbb{Q})$ are the two points in the boundary. One may check that ∞ is a torsion point, so does not affect the pairing. In order to avoid self-intersection, we apply a Hecke operator. Recall that the Hecke algebra (away from 43) is the polynomial ring

$$\mathcal{H} = \mathbb{Z}[T_p, \langle p \rangle^{\pm 1}; p \neq 43 \text{ prime}].$$

It acts on $X_0(43)$ by the correspondence

$$T_p : (A, C) \mapsto \sum_{K \subseteq A,\ |K|=p} (A/K, C \bmod K),$$

the elements $\langle p \rangle$ act as identity. We would like to pick a T_p such that $x_K \notin \operatorname{Supp} T_p(x_K)$. Thus we have to make sure that a subgroup $K \subseteq \mathbb{C}/\tau(\mathcal{I})$ of order p cannot be $\tau(O_K)$-stable. This phenomenon precisely occurs for p that are inert in K.

On the other hand, the action of $\mathcal{H}$ on $X_0(43)$ translates into a ring homomorphism

$$\mathcal{H} \to \operatorname{End}(E)$$

under which the image of T_p is precisely the p-th Fourier coefficient of the modular form corresponding to E. Looking this up in the LMFDB, we find

$$f_E(q) = q - 2q^2 - 2q^3 + 2q^4 - 4q^5 + 4q^6 + q^9 + \dots.$$

Then one may find an inert p such that also $a_p \neq 0$ and obtains

$$\widehat{h}(x_K) = a_p^{-1} \sum_{v \in \Sigma_K} \big([x_K] - [0], T_p([x_K] - [\infty])\big)_v.$$

Example 1.7. For example, $-7 \equiv 36$ is a square mod 43, so an interesting situation would be $K = \mathbb{Q}(\sqrt{-7})$. Since $-7 \equiv 2$ is not a square mod 3, one may pick T_3 with $a_p = -2$.

Interpolating this discussion, we have found an interesting intersection problem.

Problem 1.8. Let $N \geq 1$ and let $K/\mathbb{Q}$ be an imaginary-quadratic field such that there is an ideal $\mathcal{N}$ with $O_K/\mathcal{N} \cong \mathbb{Z}/N$; denote by x_K the corresponding Heegner divisor on $X_0(N)$. For suitable p, determine the intersection $(x_K, T_p(x_K))$ on the integral model of $X_0(N)$.

The answer, of course, should relate this intersection number to other quantities as in (1.3). Finally, we mention that the intersection number $\operatorname{Int}(g)$ from (0.1) precisely occurs as the length of certain local rings in $x_K \cap T_p(x_K)$.

2. The Modular Curve

Today's aim is to introduce the modular curve in a more adelic setting which will allow more elegant formulations of various results to come. The underlying mathematics is still that of elliptic curves with level-n structure from last term, however, and all statements ultimately reduce to these.

2.1. $\mathbb{Z}_p$-local systems.

Assume throughout that S is a scheme with $p \in \mathcal{O}_S^\times$. Our first task is to define the Tate module $T_p(E)$ of an elliptic curve E/S.

Definition 2.1. A $\mathbb{Z}_p$-local system over S is a commutative group scheme $\Lambda \to S$ that is of the form $\Lambda \cong \lim_{i\geq 0} \Lambda_i$ for an inverse system $(\Lambda_i)_{i\geq 1}$

$$\Lambda_1 \longleftarrow \Lambda_2 \longleftarrow \Lambda_3 \longleftarrow \dots$$

of finite étale S-group schemes that satisfies the following three assumptions.

(1) There is an integer r such that the degree of Λ_i is p^{ir}.
(2) Each map $\Lambda_{i+1} \to \Lambda_i$ is surjective. This is in the sheaf-theoretic sense for the fpqc topology, i.e. it means that $\Lambda_{i+1} \to \Lambda_i$ is faithfully flat.
(3) The kernel of each transition map is the p-torsion,

$$\ker(\Lambda_{i+1} \to \Lambda_i) = \Lambda_{i+1}[p].$$

Remark 2.2. We make some comments.

(1) Conditions (2) and (3) together allow to identify Λ_i with the image of multiplication $\mathrm{Im}([p] : \Lambda_{i+1} \to \Lambda_{i+1})$ (exercise). Taking into account (1), this image has to coincide with $\Lambda_{i+1}[p^i]$. This is why we write $[p]$ for the transition map often identify $\Lambda_i = \Lambda_{i+1}[p^i]$.
(2) The integer r is called the rank of the inverse system or of Λ. It follows as in (1) that étale locally $\Lambda_i \cong (\underline{\mathbb{Z}/p^i})^r$.
(3) Recall that inverse limits of sheaves of any kind are taken sections-wise. So, for any S-scheme U,

$$\left(\lim_{i\geq 0} \Lambda_i\right)(U) = \left\{ (x_1, x_2, \dots) \in \prod_{i\geq 1} \Lambda_i(U) \mid [p](x_{i+1}) = x_i \right\}.$$

(4) Next, note that any $\mathbb{Z}_p$-local system Λ/S is relatively affine and faithfully flat. Namely assume $S = \operatorname{Spec} R$, write $\Lambda_i = \operatorname{Spec} A_i$ for the finite locally free R-algebra $A_i = \mathcal{O}_{\Lambda_i}(\Lambda_i)$. Then $\Lambda = \operatorname{Spec} A$ with $A = \operatorname{colim}_{i\geq 1} A_i$. Since $\Lambda_{i+1} \to \Lambda_i$ is faithfully flat, each map $A_i \to A_{i+1}$ is injective and $A = \bigcup_{i\in I} A_i$ can be thought of as a union.

Example 2.3. (1) (Constant Local System) Consider $\Lambda_i = \underline{\mathbb{Z}/p^i}$ viewed as constant sheaf on S. Define the transition maps $\Lambda_{i+1} \to \Lambda_i$ as the projections. Equivalently, take $\Lambda_i = \underline{p^{-i}\mathbb{Z}/\mathbb{Z}}$ and define the transition maps as multiplication by p. Then

$$\underline{\mathbb{Z}_p} := \lim_{i\geq 1} \underline{\mathbb{Z}/p^i}$$

is the so-called constant $\mathbb{Z}_p$-local system. Assume again $S = \operatorname{Spec} R$. The occurring rings are $A_i = \prod_{z\in\mathbb{Z}/p^i\mathbb{Z}} R$, the projection $\pi : \underline{\mathbb{Z}/p^{i+1}} \to \underline{\mathbb{Z}/p^i}$ corresponds to the inclusion

$$A_i \to A_{i+1},\ (\pi^* f_i)(z) = f(\pi(z)).$$

The R-algebra A becomes

$$A = \mathrm{LC}(\mathbb{Z}_p, R) = \{f : \mathbb{Z}_p \to R \text{ locally constant map.}\}.$$

In particular, one finds (exercise) that the functor of points is that of continuous maps to the profinite set $\mathbb{Z}_p$ from the underlying topological space,

$$\underline{\mathbb{Z}_p}(U) = \mathrm{Cont}(U, \mathbb{Z}_p).$$

(2) (Tate Twists). Consider $\Lambda_i = \mu_{p^i}$ with transition map $\Lambda_{i+1} \to \Lambda_i$ is $x \mapsto x^p$. The resulting local system is called the (first) Tate twist $\underline{\mathbb{Z}_p}(1)$,

$$\underline{\mathbb{Z}_p}(1) := \lim_{i\geq 1} \mu_{p^i} = \mathrm{Spec}\, \mathcal{O}_S[\zeta_p, \zeta_{p^2}, \ldots]/(\zeta_p^p - 1, \zeta_{p^2}^p - \zeta_p, \ldots).$$

(3) (Tate modules) Let E/S be an elliptic curve. Take $\Lambda_i = E[p^i]$ with transition map $[p] : E[p^{i+1}] \to E[p^i]$. This defines its Tate module, a $\mathbb{Z}_p$-local system of rank 2,

$$T_p(E) := \lim_{i\geq 1} E[p^i].$$

(4) (General case) Every inverse system $(\Lambda_i)_{i\geq 1}$ as above is fpqc locally isomorphic to the constant local system. Namely we find finite étale coverings $\ldots \to S_2 \to S_1 \to S$ such that $S_i \times_S \Lambda_i \cong (\underline{\mathbb{Z}/p^i})^r$. Then we may consider the fpqc covering $\lim_{i\geq 1} S_i \to S$. It follows that every $\underline{\mathbb{Z}_p}$-local system is fpqc locally isomorphic to the constant one of the same rank $\underline{\mathbb{Z}_p}^r$.

Definition 2.4. Let X be a locally profinite set and S a scheme. Then we define the following functor on S-schemes,

$$\underline{X}_S(U) := \mathrm{Cont}(U, X).$$

Exercise: Show that $\underline{X}_S$ is representable by an S-scheme. It is affine over S if X is profinite.

We now give further properties and definitions of local systems. Whenever we take a quotient or colimit, it is meant in the sense of fpqc sheaves. We use the terminology of Def. 2.1 throughout.

(1) Every $\mathbb{Z}_p$-local system is p-torsion free. Namely

$$p(x_1, x_2, \ldots) = (px_1, px_2, \ldots) = (0, x_1, x_2, \ldots)$$

vanishes if and only if all $x_i = 0$.

(2) There is a map $\Lambda \to \Lambda_i$ given by projection to the i-th coordinate. Its kernel is $p^i\Lambda$, which is isomorphic to Λ by (1). We obtain $\Lambda_i = \Lambda/p^i\Lambda$ and, in particular, the canonical presentation $\Lambda = \lim_{i\geq 1} \Lambda/p^i\Lambda$.

(3) Let Λ, Λ' be two $\mathbb{Z}_p$-local systems and let $f : \Lambda \to \Lambda'$ be a map of S-group schemes. Then we obtain compatible maps $(f_i : \Lambda/p^i\Lambda \to \Lambda'/p^i\Lambda')_{i\geq 1}$ and, conversely, any such tuple (f_i) defines a map $\Lambda \to \Lambda'$. In other words,

$$\mathrm{Hom}(\Lambda, \Lambda') = \lim_{i\geq 1} \mathrm{Hom}(\Lambda/p^i\Lambda, \Lambda'/p^i\Lambda').$$

In particular, the Hom-functor of two $\mathbb{Z}_p$-local systems,

$$\underline{\mathrm{Hom}}(\Lambda, \Lambda')(U) := \mathrm{Hom}(U \times_S \Lambda, U \times_S \Lambda'),$$

is itself a $\mathbb{Z}_p$-local system of rank $\mathrm{rk}(\Lambda)\mathrm{rk}(\Lambda')$, namely equal to $\lim_{i\geq 1} \underline{\mathrm{Hom}}(\Lambda/p^i\Lambda, \Lambda'/p^i\Lambda')$.

(4) Just like with usual finite free $\mathbb{Z}_p$-modules, a map $f : \Lambda \to \Lambda'$ is an isomorphism if and only if $f_1 : \Lambda/p\Lambda \to \Lambda'/p\Lambda'$ is. To prove this (exercise), use induction on the exact sequences

$$0 \to \Lambda_1 \to \Lambda_{i+1} \to \Lambda_i \to 0, \qquad 0 \to \Lambda'_1 \to \Lambda'_{i+1} \to \Lambda'_i \to 0.$$

(5) The isomorphism functor $\underline{\mathrm{Isom}}(\Lambda, \Lambda')$ (in particular also $\underline{\mathrm{Aut}}(\Lambda)$) is similarly representable by an affine group scheme, namely $\lim_{i\geq 1} \underline{\mathrm{Isom}}(\Lambda_i, \Lambda'_i)$. It is an open subscheme

of $\underline{\mathrm{Hom}}(\Lambda, \Lambda')$ with group structure given by composition. We will need this later for the trivial local system of rank 2, here

$$\underline{\mathrm{Aut}}(\underline{\mathbb{Z}_p^2}) = \lim_{i \geq 1} \underline{GL_2(\mathbb{Z}/p^i)} = \underline{GL_2(\mathbb{Z}_p)}.$$

Definition 2.5. A $\mathbb{Q}_p$-local system over S is a group scheme $V \to S$ that is of the form $\Lambda[p^{-1}]$ for some $\mathbb{Z}_p$-local system $\Lambda \to S$.

We remark that, for every $\mathbb{Z}_p$-local system Λ, the group functor $\Lambda[p^{-1}]$ obtained by inverting p is again representable. Thus $\Lambda[p^{-1}]$ is a $\mathbb{Q}_p$-local system. The representing scheme is obtained as the infinite union of copies of Λ along the open immersions $[p] : \Lambda \hookrightarrow \Lambda$. This is just like the description $\mathbb{Q}_p = \bigcup_{n \geq 0} p^{-n}\mathbb{Z}_p$.

The Hom-functors and Isom-functors for $\mathbb{Q}_p$-local systems are also representable. For the constant $\mathbb{Q}_p$-local system, obtained as $\underline{\mathbb{Q}_p} := \underline{\mathbb{Z}_p}[p^{-1}]$, these become

$$\underline{\mathbb{Q}_p}(U) = \mathrm{Cont}(U, \mathbb{Q}_p), \quad (\underline{\mathrm{Aut}}(\underline{\mathbb{Q}_p^2}))(U) = \underline{GL_2(\mathbb{Q}_p)}.$$

2.2. **Elliptic Curves up to isogeny.** Continue to assume $p \in \mathcal{O}_S^\times$.

Definition 2.6. Let V be a $\mathbb{Q}_p$-local system over S. A lattice in V is a subsheaf $\Lambda \subseteq V$ that is a $\mathbb{Z}_p$-local system and satisfies $\Lambda[p^{-1}] = V$.

Given an elliptic curve E/S, its Tate module $T_p(E)$ inside the rational Tate module $V_p(E) := T_p(E)[p^{-1}]$ is a lattice. An isogeny $\varphi : E \to E'$ defines an isomorphism $\varphi : V_p(E) \cong V_p(E')$ and hence a lattice $\varphi(T_p(E)) \subset V_p(E')$.

We write $\mathcal{E}\ell\ell(S)$ for the category of elliptic curves over S. Define a second category $\mathcal{E}(S)$ as follows. Its objects are pairs (E, Λ) of an elliptic curve E and a lattice $\Lambda \subseteq V_p(E)$. Its morphisms are[2]

$$\mathrm{Hom}\big((E, \Lambda), (E', \Lambda')\big) = \{x \in \mathrm{Hom}(E, E')[p^{-1}] \mid x\Lambda \subseteq \Lambda'\}.$$

Proposition 2.7. *There is an equivalence of categories, functorial in S,*

$$\begin{aligned} \mathcal{E}\ell\ell(S) &\xrightarrow{\cong} \mathcal{E}/S \\ E &\longmapsto (E, T_p(E)). \end{aligned} \tag{2.1}$$

Proof. One may reduce to S quasi-compact, which we assume from now on. *Fully Faithfulness.* We need to show that an element $x' \in \mathrm{Hom}(E, E')[p^{-1}]$ lies in $\mathrm{Hom}(E, E')$ if it satisfies $xT_p(E) \subseteq T_p(E')$. A priori, we only know $p^n x \in \mathrm{Hom}(E, E')$ for large n and, in particular $p^n x T_p(E) \subseteq T_p(E')$. Then

$$\begin{aligned} xT_p(E) \subseteq T_p(E') &\Leftrightarrow \big(p^n x : T_p(E)/p^n T_p(E) \longrightarrow T_p(E')/p^n T_p(E')\big) = 0 \\ &\Leftrightarrow \big(p^n x : E[p^n] \to E'[p^n]\big) = 0 \\ &\Leftrightarrow p^n x \text{ divisible by } p^n \\ &\Leftrightarrow x \in \mathrm{Hom}(E, E'). \end{aligned}$$

Essential Surjectivity. Given a pair (E, Λ), we need to find an isomorphic pair $(E', T_p(E'))$. Isomorphic in $\mathcal{E}$ means there exists an invertible element $x \in \mathrm{Hom}(E, E')[p^{-1}]$ such that $x\Lambda = T_p(E')$. Invertible means that the degree of x, a locally constant function with values in $\mathbb{Z}[p^{-1}]_{\geq 0}$, lies in $p^{\mathbb{Z}}$. First note that $[p^n]$ gives an isomorphism $(E, \Lambda) \cong (E, p^n\Lambda)$ for all $n \in \mathbb{Z}$. So we may assume $\Lambda \subseteq T_p(E)$. Pick m with $p^m T_p(E) \subseteq \Lambda$. This defines

[2] To be completely correct, one has to sheafify $\mathrm{Hom}(E, E')[p^{-1}]$ here for non-quasi-compact S. In other words, one has to allow the denominator to be globally unbounded.

a subgroup $K := \Lambda/p^m T_p(E) \subseteq T_p(E)/p^m T_p(E) = E[p^m]$. Consider the quotient isogeny $x : E \to E' = E/K$. Its (locally constant) degree $|K|$ is a power of p, so x is an invertible element of $\mathrm{Hom}(E, E')[p^{-1}]$. Then $x\Lambda \subseteq p^m T_p(E')$ by construction. Moreover, for any isogeny $x : E \to E'$ of elliptic curves, just from definitions,

$$x^{-1}(E'[p]) = [p]^{-1} \ker(x),$$

which provides $x : \Lambda/p\Lambda \cong p^m T_p(E')/p^{m+1}T_p(E')$. This implies $x\Lambda = p^m T_p(E')$. Thus

$$(E, \Lambda) \cong (E', p^m T_p(E')) \underset{[p^{-m}]}{\cong} (E', T_p(E')).$$

□

2.3. **The Modular Curve.** Let $B \in \mathbb{Z}$ be an integer. We work with schemes over $\mathbb{Z}[B^{-1}]$ in the following. Write

$$\mathbb{Z}_B := \prod_{p|B} \mathbb{Z}_p, \quad \mathbb{Q}_B := \prod_{p|B} \mathbb{Q}_p = \mathbb{Z}_B[B^{-1}].$$

The definition of $\mathbb{Z}_B$-local systems and $\mathbb{Q}_B$-local systems is just as before, they are in fact products of the p-adic versions, for $p \mid B$. Fix an open compact subgroup $K \subseteq GL_2(\mathbb{Q}_B)$, the so-called level. For example, K might be the principal congruence subgroup of level n,

$$K(n) := \ker\big(GL_2(\mathbb{Z}_B) \to GL_2(\mathbb{Z}/n)\big).$$

(Here we assume that $n \in \mathbb{Z}[B^{-1}]^\times$, i.e. n has only prime factors dividing B.) The principal congruence subgroups form a neighborhood basis of the identity in $GL_2(\mathbb{Q}_B)$, so every K contains some $K(n)$.

Definition 2.8. Let $\mathcal{M}_K(S)$ denote the groupoid of elliptic curves with level-K-structure over S. These are defined as pairs $(E, \bar\eta)$, where E/S is an elliptic curve and $\bar\eta$ a K-orbit of isomorphisms

$$\eta : \underline{\mathbb{Q}_B}^2 \xrightarrow{\cong} V_p(E).$$

An isomorphism of two such tuples $(E, \bar\eta) \cong (E', \bar\eta')$ is an isomorphism $\gamma \in \mathrm{Hom}(E, E')[B^{-1}]$ such that $\gamma \circ \bar\eta = \bar\eta'$. Isomorphism means that there is some $\gamma^{-1} \in \mathrm{Hom}(E', E)[B^{-1}]$. This is equivalent to $\deg(\gamma)$, which is a locally constant function on S with values in $\mathbb{Z}[B^{-1}]_{\geq 0}$, to take values in $\mathbb{Z}[B^{-1}]^\times$.

This is a subtle definition and we now explain it in detail. First, we provide a precise definition of K-orbit of isomorphisms. We have seen in §2.1 that there is a scheme $\underline{\mathrm{Isom}}(\underline{\mathbb{Q}_B^2}, V_B(E))$ that parametrizes isomorphisms from the constant $\mathbb{Q}_B$-local system to the rational Tate module of E. We have also seen the explicit description

$$\underline{\mathrm{Aut}}(\underline{\mathbb{Q}_B^2})(-) = \underline{GL_2(\mathbb{Q}_B)}.$$

It acts on $\underline{\mathrm{Isom}}(\underline{\mathbb{Q}_B^2}, V_B(E))$ by composition and contains $\underline{K}$ as subgroup scheme. A K-orbit of isomorphisms is then a section of the quotient

$$\bar\eta \in \Big(\underline{\mathrm{Isom}}(\underline{\mathbb{Q}_B^2}, V_B(E))/\underline{K}\Big)(S). \tag{2.2}$$

Here, the occurring quotient is taken in the sense of fpqc sheaves. It is itself an étale scheme over S. Namely, after base change to an fpqc covering $S' \to S$, it becomes isomorphic to the constant scheme

$$\underline{\mathrm{Isom}}(\underline{\mathbb{Q}_B^2}, \underline{\mathbb{Q}_B^2})/\underline{K} = \underline{GL_2(\mathbb{Q}_B)}/\underline{K} = \underline{GL_2(\mathbb{Q}_B)/K}.$$

The following provides an explicit description.

Example 2.9. Let E/k be an elliptic curve over a field k with $\mathrm{char}(k) \nmid B$, write $G = \mathrm{Gal}(\overline{k}/k)$. Recall that étale $X \to \operatorname{Spec} k$ are the same as (discrete) sets with continuous G-action. This bijection is given by $X \mapsto X(\overline{k})$. Taking limits, there is an equivalence of categories

$$\begin{aligned} \{\mathbb{Z}_p\text{-local systems over } \operatorname{Spec} k\} &\cong \left\{\begin{smallmatrix}\text{continuous } G\text{-representations} \\ \text{on finite free } \mathbb{Z}_p\text{-modules}\end{smallmatrix}\right\} \\ \Lambda &\longmapsto \Lambda(\overline{k}). \end{aligned} \tag{2.3}$$

This verbatim applies to $\mathbb{Q}_p$-local systems. The quotient $\underline{\mathrm{Isom}}(\underline{\mathbb{Q}_B^2}, V_p(E))/\underline{K}$ in (2.2) is the étale scheme of the G-set $\mathrm{Isom}(\mathbb{Q}_B^2, V_p(E)(\overline{k}))/K$.[3]

We now link the new definition of level structure with the classical one. Let $\mathcal{E}\ell\ell_n$ denote the groupoid-valued functor

$$\mathcal{E}\ell\ell_n(S) = \{(E, \alpha) \mid E/S \text{ an EC}, \ \alpha : (\mathbb{Z}/n)^2 \cong E[n] \text{ a level-}n\text{-structure}\}.$$

Proposition 2.10. *For each $n \in \mathbb{Z}[B^{-1}]^\times$, there are equivalences, functorial in S,*

$$\mathcal{M}_{K(n)}(S) \cong \mathcal{E}\ell\ell_n(S).$$

Note before the proof that isomorphisms of pairs $(E, \bar{\eta})$ and $(E', \bar{\eta}')$ may come from $\mathrm{Hom}(E, E')[B^{-1}]$ while isomorphisms of pairs (E, α) and (E', α') have to lie in $\mathrm{Hom}(E, E')$. This has to play a crucial role in the proof of course, since the quotient in (2.2) is infinite while an elliptic curve only admits finitely many classical level-n-structures.

Proof. Step 1: The case $n = 1$. Then $K = GL_2(\mathbb{Z}_B)$ and our claim is that a K-orbit $\bar{\eta}$ is the same as a $\mathbb{Z}_B$-lattice $\Lambda \subseteq V_B(E)$. Namely let $S' \to S$ be an fpqc covering such that there exists an $\eta \in \bar{\eta}_{S'}$. We associate to it the lattice $\Lambda := \eta(\underline{\mathbb{Z}_B^2})$. Over $S'' := S' \times_S S'$, the two pullbacks $p_1^*\eta$ and $p_2^*\eta$ satisfy

$$p_1^*\eta = p_2^*\eta \circ g, \quad \text{some unique } g : S'' \to K,$$

because the quotient class $\bar{\eta}$ is defined over S. But $g\underline{\mathbb{Z}_B^2} = \underline{\mathbb{Z}_B^2}$, so $p_1^*\Lambda = p_2^*\Lambda$ and hence Λ is defined over S.

Assume conversely that we are given a $\mathbb{Z}_B$-lattice $\Lambda \subset V_B(E)$. Every $\mathbb{Z}_B$-local system is fpqc locally constant, so we find an fpqc covering $S' \to S$ and an isomorphism $\eta : \underline{\mathbb{Z}_B^2} \cong \Lambda_{S'}$. Over $S'' = S' \times_S S'$, we obtain two isomorphisms $p_1^*\eta, p_2^*\eta : \underline{\mathbb{Z}_B^2} \to \Lambda_{S''}$. They differ by an automorphism of $\underline{\mathbb{Z}_B^2}$ over S'', i.e. a continuous map $g : S'' \to K$. Thus the K-orbit $\eta K \in (\mathrm{Isom}(\underline{\mathbb{Q}_B^2}, V_B(E))/\underline{K})(S')$ is defined over S.

In this way, we constructed from $(E, \bar{\eta})$ some $(E, \Lambda) \in \mathcal{E}(S)$. Then we apply Prop. 2.7.

Step 2: Case of general n. Now let $K = K(n)$. Given a pair $(E, \bar{\eta}) \in \mathcal{M}_K(S)$, we first consider the coarser datum $(E, \bar{\eta} \cdot \underline{GL_2(\mathbb{Z}_B)})$. Step 1 (and the proof of Prop. 2.7) showed that we find an invertible element $\gamma \in \mathrm{Hom}(E, E')[B^{-1}]$ such that

$$(\gamma \circ \eta)(\underline{\mathbb{Z}_B^2}) = T_p(E'), \quad \eta \in \bar{\eta} \text{ any.}$$

Replacing $(E, \bar{\eta})$ by this isomorphic pair $(E', \gamma \circ \bar{\eta})$, we may assume $\bar{\eta}(\underline{\mathbb{Z}_B^2}) = T_B(E)$. Let a, b be the standard basis of $\underline{\mathbb{Z}_B^2}$. Take some fpqc covering $S' \to S$ such that there exists $\eta \in \bar{\eta}_{S'}$ and write

$$\eta(a) = (x_1, x_2, \ldots), \quad \eta(b) = (y_1, y_2, \ldots).$$

[3] The equivalence (2.3) and the given description of $\underline{\mathrm{Isom}}(\underline{\mathbb{Q}_B^2}, V_B(E))/\underline{K}$ carry over to arbitrary connected scheme S, using the formalism of étale fundamental groups.

Here, by definition, $x_i, y_i \in E[B^i](S')$. Now one works prime-by-prime and we assume $n = p^r$ for simplicity. Then η being an isomorphism for sure implies η mod p^r to be an isomorphism as well, so $\alpha := (x_r, y_r)$ defines a level-p^r-structure of E over S'.

We still need to see that x_r and y_r lie in $E(S)$. But $p_1^*\eta = p_2^*\eta g$ for some $g : S'' \to K(n)$, and thus

$$p_1^* x_r = (p_1^*\eta)(a) = (p_2^*\eta)(a) = p_2^* x_r$$

and analogously for y_r. Thus α is defined over S and we have constructed a functor $\mathcal{M}_{K(n)}(S) \to \mathcal{E}\ell\ell_n(S)$.

Faithfulness of the functor is immediate. For the fullness, consider two pairs $(E, \bar\eta), (E', \bar\eta') \in \mathcal{M}_{K(n)}(S)$. Up to replacing by isomorphic pairs, we may assume $\bar\eta(\underline{\mathbb{Z}_B^2}) = T_B(E)$ and $\bar\eta'(\underline{\mathbb{Z}_B^2}) = T_B(E')$. Let α and α' denote the two constructed level-n-structures for E and E' and let $\gamma \in \mathrm{Isom}(E, E')$ be such that $\alpha = \gamma\alpha'$. This means that $(\eta(a), \eta(b)) = (\gamma\eta'(a), \gamma\eta'(b))$ modulo n whenever $\eta \in \bar\eta_{S'}$ and $\eta' \in \bar\eta'_{S'}$. In other words, $(\gamma\eta')^{-1}\eta \in K(n)(S')$ which means that γ defines an isomorphism $\gamma : (E, \bar\eta) \cong (E, \bar\eta')$.

Essential surjectivity, finally, is the statement that every level-n-structure can be lifted to a full level structure $\eta : \underline{\mathbb{Z}_B^2} \cong T_B(E)$ after passing to an fpqc covering. This we leave as an exercise. □

In order to understand general groups K, we next note the following two functorialities.

(1) If $K' \subseteq K$, then there is a projection map

$$\mathcal{M}_{K'} \to \mathcal{M}_K,\ (E, \bar\eta) \mapsto (E, \bar\eta \cdot \underline{K}).$$

(2) For every $g \in GL_2(\mathbb{Q}_B)$, there is an isomorphism

$$\mathcal{M}_K \cong \mathcal{M}_{g^{-1}Kg},\ (E, \bar\eta) \mapsto (E, \bar\eta g). \tag{2.4}$$

The group $GL_2(\mathbb{Z}_B) \subseteq GL_2(\mathbb{Q}_B)$ is maximal with respect to inclusion of compact subgroups. (It is not unique with this property, any conjugate $g^{-1}GL_2(\mathbb{Z}_B)g$ is similarly maximal compact.) Moreover, for every open compact $K \subseteq GL_2(\mathbb{Q}_B)$, there exists g such that $g^{-1}Kg \subseteq GL_2(\mathbb{Z}_B)$.

Theorem 2.11. *Assume that some conjugate of K is contained in some subgroup $K(m)$ with $m \geq 3$. Then the functor $\mathcal{M}_K$ is representable by a smooth affine $\mathbb{Z}[B^{-1}]$-scheme of relative dimension* 1.

Remark 2.12. Strictly speaking, each $\mathcal{M}_K(S)$ is a groupoid. But under the given assumption on K, each $\mathcal{M}_K(S)$ is equivalent to a set, meaning that the only automorphisms of objects are the identity. This set may be chosen as the set of isomorphism classes $\mathcal{M}_K(S)/\cong$ and Thm. 2.11 more precisely means $S \longmapsto \mathcal{M}_K(S)/\cong$ is representable.

Proof. Using the isomorphism (2.4), we may assume that $K \subseteq K(m)$. Since K is open, there is some n with $K(n) \subseteq K$. Since $K(n)$ is normal in $GL_2(\mathbb{Z}_B)$, it is also normal in K and we define $\bar K := K/K(n)$. It acts on $\mathcal{M}_{K(n)}$ by $(E, \bar\eta) \cdot g := (E, \bar\eta g)$. (This is again the isomorphism (2.4), but $K = g^{-1}Kg$ because of normality.) We know from the last course that $\mathcal{M}_{K(n)} \cong \mathcal{E}\ell\ell_n$ is representable by a smooth affine scheme of relative dimension 1. Because $K \subseteq K(m)$ with $m \geq 3$, the $\bar K$-action on it is free. The quotient $\mathcal{M}_{K(n)}/\bar K$ then represents $\mathcal{M}_K$. □

3. CM Cycles

3.1. **Group-theoretic definition.** We first explain where CM cycles come from group-theoretically. This is for motivation and understanding only, we will work with a moduli-theoretic definition later. Let

$$K^\circ := K \times \prod_{p \nmid B} GL_2(\mathbb{Z}_p) \subset GL_2(\mathbb{A}_f)$$

denote the completed level where we filled in the standard group at all primes $p \nmid B$. Last term we essentially saw that the modular curve of level K we just defined has complex points

$$\mathcal{M}_K(\mathbb{C}) = GL_2(\mathbb{Q}) \backslash \left(\mathbb{H}^\pm \times GL_2(\mathbb{A}_f)/K^\circ \right)$$

where $\mathbb{H}^\pm = \mathbb{C} \backslash \mathbb{R}$ is two copies of the upper half plane. Let $L/\mathbb{Q}$ be an imaginary-quadratic field and fix an embedding $L \to M_2(\mathbb{Q})$. (This is the same as defining an L-vector space structure on $\mathbb{Q}^2$.) We write $T = \mathrm{Res}_{L/\mathbb{Q}}(\mathbb{G}_m)$ for the torus of L. More precisely, this is the (two-dimensional, commutative, smooth) group scheme over $\mathbb{Q}$ with

$$T(R) = (R \otimes_{\mathbb{Q}} L)^\times .$$

(It is called a torus because $L \otimes_{\mathbb{Q}} T \cong \mathbb{G}_m^2$.) Then $T(\mathbb{Q}) \subseteq GL_2(\mathbb{Q})$ acts on $\mathbb{H}^\pm$ by Moebius transformations. This action has two fixed points, one on each connected component of $\mathbb{H}$. We pick one, say x. This constructs a map

$$T(\mathbb{Q}) \backslash \left(\{x\} \times T(\mathbb{A}_f)/(T(\mathbb{A}_f) \cap K^\circ) \right) \longrightarrow GL_2(\mathbb{Q}) \backslash \left(\mathbb{H}^\pm \times GL_2(\mathbb{A}_f)/K^\circ \right).$$

Note that the domain is a finite set. Tracing through definitions, one can work out that the image is a set of elliptic curves with complex multiplication by L and L-linear level-K-structure.

3.2. **Moduli-theoretic definition.** We continue to fix some $B \in \mathbb{Z}$ and a level group $K \subseteq \prod_{p|B} GL_2(\mathbb{Q}_p)$. Let $L/\mathbb{Q}$ be imaginary-quadratic, write $T = \mathrm{Res}_{L/\mathbb{Q}}(\mathbb{G}_m)$, fix an embedding $L \to M_2(\mathbb{Q})$. Assume that $O_L[B^{-1}]$ stabilizes the lattice $\mathbb{Z}[B^{-1}]^2 \subseteq \mathbb{Q}^2$. We work with schemes over $O_L[B^{-1}]$. Write $L_B = \prod_{p|B} L_p$, where L_p is the p-adic completion of L.

Definition 3.1. Let S be an O_L-scheme. The S-valued points of the CM cycle for the above data is the groupoid

$$\mathcal{C}_K(S) = \{(E, \iota, \bar{\eta})\}$$

where the triples are as follows.

(1) E/S is an elliptic curve.
(2) $\iota : O_L[B^{-1}] \to \mathrm{End}(E)[B^{-1}]$ is an action that satisfies the following condition. Every $a \in O_L[B^{-1}]$ acts on the Lie algebra $\mathrm{Lie}(E)$ through the structure map $O_L[B^{-1}] \to \mathcal{O}_S$,
$$(a|\,\mathrm{Lie}(E)) = a \quad \text{as elements of } \mathrm{End}(\mathrm{Lie}(E)) = \mathcal{O}_S. \tag{3.1}$$
This an example of the famous Kottwitz condition.
(3) $\bar{\eta}$ is a $K \cap T(\mathbb{Q}_B)$-orbit of isomorphisms $\eta : L_B \cong V_B(E)$. Here, both sides are viewed as $\mathbb{Q}_B$-local system of rank 2 with L-action.

To define a groupoid resp. a set of isomorphism classes, we also have to explain what the isomorphisms $\gamma : (E, \iota, \bar{\eta}) \to (E', \iota', \bar{\eta}')$ are. These are invertible $\gamma \in \mathrm{Hom}(E, E')[B^{-1}]$ that are L-linear (i.e. $\gamma \circ \iota(a) = \iota'(a) \circ \gamma$ for all a) and respect the level structure, $\gamma \circ \bar{\eta} = \bar{\eta}'$.

Imposing the Kottwitz condition (3.1) corresponds to the choice of one of the two fixed points of $T(\mathbb{Q})$ on $\mathbb{H}^\pm$ in §3.1.

Definition 3.2. The forgetful map to the modular curve is given by

$$\mathcal{C}_K(S) \longrightarrow \mathcal{M}_K(s)$$
$$(E, \iota, \bar{\eta}) \longmapsto (E, \bar{\eta}K).$$

We next show that $\mathcal{C}_K$ is representable, then we examine its properties.

3.3. **Representability.**

Theorem 3.3. *Let $E, E'/S$ be two elliptic curves. The Hom-functor on schemes over S,*

$$\underline{\mathrm{Hom}}(E, E')(U) := \mathrm{Hom}(U \times_S E, U \times_S E')$$

is representable by an unramified S-scheme that is a union of projective S-schemes.

Proof. We may assume S noetherian by approximation.

(1) To any map $\phi : U \times_S E \to U \times_S E'$ of U-schemes we may associate its graph $\Gamma_\phi \subseteq U \times_S (E \times_S E')$. It is a closed subscheme (by separatedness of E'/S) with the property that the first projection restricts to an isomorphism

$$p_1|_{\Gamma_\phi} : \Gamma_\phi \xrightarrow{\cong} U \times_S E.$$

Conversely, given a closed subscheme $\Gamma \subset U \times_S (E \times_S E')$ such that $p_1|_\Gamma$ is an isomorphism, we obtain the map $\phi_\Gamma := p_2 \circ (p_1|_\Gamma)^{-1} : U \times_S E \to U \times_S E'$.

(2) Because of this, we consider the Hilbert scheme $H := \mathrm{Hilb}_{E \times_S E'/S}$. It is the functor (over S) with points

$$H(U) = \left\{ Z \subseteq U \times_S (E \times_S E') \,\middle|\, \begin{array}{l} Z \text{ closed subscheme of locally finite} \\ \text{presentation s.th. } Z \to U \text{ is flat} \end{array} \right\}$$

By a theorem of Grothendieck, this functor is representable by an S-scheme that is a union of projective S-schemes. (See [2, no. 221, Thm. 3.1] or [4, §5]; alternatively [10, Tag 0D01] which only states representability as algebraic space however.)

(3) Let from now on $Z \subset H \times_S (E \times_S E')$ denote the universal closed subscheme and consider the first projection

$$p_1|_Z : Z \longrightarrow H \times_S E.$$

By semi-continuity of fiber dimension, there is a maximal closed subscheme $Q \subseteq H \times_S E$ over which fibers are of dimension ≥ 1. (In fact of dimension precisely 1 because they are subschemes of E'.) The image $p_H(Q) \subseteq H$ is closed by properness, denote by V its complement. Thus $Z \cap (V \times_S \times (E \times_S E'))$ is the universal closed subscheme that is finite over $V \times_S E$.

(4) Consider the map on sheaves of rings,

$$\psi : \mathcal{O}_{V \times_S E} \longrightarrow p_{1,*}\mathcal{O}_{Z \cap (V \times_S (E \times_S E'))}.$$

The target is a finite presentation $\mathcal{O}_{V \times_S E}$-module, so $\mathrm{Supp}(\mathrm{Coker}(\psi)) \subseteq V \times_S E$ is closed. Its image under p_V in V is closed by properness, let $V' \subseteq V$ denote its complement. Then V' is the locus in H where $p_1|_Z$ is a closed immersion.

(5) Now $\mathcal{F} := p_{1,*}\mathcal{O}_{Z \cap (V' \times_S E)}$ is a quotient of $\mathcal{O}_{V' \times_S E}$. The locus $Q' \subseteq V' \times_S E$ where $\mathcal{F}$ is not flat over $\mathcal{O}_{V' \times_S E}$ is a closed subset. Put

$$V'' := V' \setminus \left(p_{V'}(Q')\right)$$

which is open by properness of E. One can now check that $V'' \subseteq H$ precisely parametrizes graphs of scheme morphisms $\phi : E \to E'$ (detail omitted, cf. [4, Thm. 5.22]).

(6) Finally, we only want to consider group scheme homomorphisms. Let $\phi : E_{V''} \to E'_{V''}$ be the universal scheme morphism. Then

$$\underline{\mathrm{Hom}}(E, E') = V'' \times_{e',\, E'_{V''},\, \phi\circ e} V''$$

where $e \in E$ and $e' \in E'$ denote the two identity elements. (Recall that a map of elliptic curves is a group homomorphism if and only if it preserves identity sections by the rigidity lemma.) This finishes the proof of representability of $\underline{\mathrm{Hom}}(E, E')$ by a union of quasi-projective S-schemes.

(7) We have seen that $\underline{\mathrm{Hom}}(E, E')$ satisfies the valuative criterion of properness last term (Weil extension theorem). Thus $\underline{\mathrm{Hom}}(E, E')$ is a union of projective S-schemes. We have also seen unramifiedness, which follows from the rigidity lemma. The proof is complete. □

Corollary 3.4. *Assume that K contains a conjugate of some $K(m)$ with $m \geq 3$. Then $\mathcal{C}_K$ is representable by a scheme. The morphism*

$$\mathcal{C}_K \longrightarrow O_L[B^{-1}] \otimes_{\mathbb{Z}[B^{-1}]} \mathcal{M}_K$$

is finite and unramified.

Proof. (1) Pick some generator $O_L = \mathbb{Z}[\zeta]$. The characteristic polynomial of ζ is irreducible, its coefficients are $\zeta + \bar{\zeta}$ and $\zeta\bar{\zeta}$. Giving an action $\iota : O_L \to \mathrm{End}(E)$ is the same as specifying an element $x = \iota(\zeta) \in \mathrm{End}(E)$ that satisfies the same characteristic polynomial, which amounts to it having the same trace and norm as ζ, i.e.

$$x + x^* = [\zeta + \bar{\zeta}], \quad xx^* = [\zeta\bar{\zeta}].$$

We have written $[\zeta + \bar{\zeta}]$ and $[\zeta\bar{\zeta}]$ here to indicate that here we consider these integers in $\mathbb{Z} \subseteq \mathrm{End}(E)$.

(2) Consider now the universal pair $(\mathcal{E}, \bar{\eta})/\mathcal{M}_K$ and apply Thm. 3.3. Trace and norm define a morphism of schemes

$$\begin{aligned} \underline{\mathrm{End}}(E)[B^{-1}] &\longrightarrow \underline{\mathbb{Z}[B^{-1}] \times \mathbb{Z}[B^{-1}]} \\ x &\longmapsto (x + x^*, xx^*). \end{aligned}$$

Let $X \subseteq \underline{\mathrm{End}}(E)[B^{-1}]$ denote the fiber above $(\zeta + \bar{\zeta}, \zeta\bar{\zeta})$. It parametrizes $O_L[B^{-1}]$-actions.

(3) Let $(\mathcal{E}, \iota, \bar{\eta})$ be the universal triple over X. Consider the map of quotients

$$\underline{\mathrm{Isom}}_{L_B}(\underline{L_B}, V_B(\mathcal{E}))/\underline{T(\mathbb{Q}_B) \cap K} \longrightarrow \underline{\mathrm{Isom}}_{\mathbb{Q}_B}(\underline{L_B}, V_B(\mathcal{E}))/\underline{K}. \tag{3.2}$$

It is a morphism of étale X-schemes. The fiber over $\bar{\eta}$ is representable by an étale scheme $X' \to X$. In fact, $X' \subseteq X$ is an open and closed subscheme. Namely if there exists some L-linear $\eta \in \bar{\eta}$, then every other such L-linear isomorphism differes by $T(\mathbb{Q}_B) \cap K$. This shows injectivity of (3.2).

(4) Let $(\mathcal{E}, \iota, \bar{\eta})$ be the universal triple over X'. (Now $\bar{\eta}$ is an orbit of L-linear isomorphisms as in Def. 3.1.) Then

$$(\iota(\zeta) | \mathrm{Lie}(\mathcal{E})) - \zeta \in \mathrm{End}(\mathrm{Lie}(\mathcal{E})) = \mathcal{O}_{X'}$$

is some element that measures the failure of the Kottwitz condition (3.1). It generates an ideal sheaf $\mathcal{I} \subseteq \mathcal{O}_{X'}$ and we find

$$\mathcal{C}_K = V(\mathcal{I}) \subseteq X'$$

which finishes the proof of representability.

(5) Unramifiedness of $\mathcal{C}_K \to \mathcal{M}_K$ is again the rigidity lemma. Getting finiteness is a little tricky, however. Given an elliptic curve $E/\operatorname{Spec} k$ over a field, we have classified the possibilities of $\mathrm{End}(E)$: It is either $\mathbb{Z}$, an order in an imaginary-quadratic extension of $\mathbb{Q}$

or an order in a definite quaternion division algebra. These are positive definite quadratic lattice for the form $q(x) = \deg(x)$ and hence only have finitely many elements of degree $\zeta\bar{\zeta}$. This shows quasi-finiteness. Getting the general statement is a little tricky: Even though we now know $\mathcal{C}_K \to \mathcal{M}_K$ to be locally finite type, to be quasi-finite and to satisfy the valuative criterion of properness, we lack quasi-compactness. One possible argument would be to use that the locus in the Hilbert scheme where the Hilbert polynomial is fixed is projective [2, no. 221, Thm. 3.2] (omitted). □

3.4. **Finiteness of $\mathcal{C}_K$.** Now we turn to properties of $\mathcal{C}_K \to \operatorname{Spec} O_L[B^{-1}]$.

Theorem 3.5. *Assume K is contained in the conjugate of some $K(m)$ for $m \geq 3$. The morphism of schemes*

$$\mathcal{C}_K \longrightarrow \operatorname{Spec} O_L[B^{-1}]$$

is finite and étale.

We prove finiteness first and étaleness in the next section. For both statements we first introduce some general machinery that applies to abelian varieties more generally. Before doing so, we give an example to demonstrate why both properties are quite remarkable.

Example 3.6. (1) Consider $V(xy-1) \subseteq \mathbb{A}^2$. It is a closed subscheme, so in particular finite and unramified "over" $\mathbb{A}^2$ just like $\mathcal{C}_K \to \mathcal{M}_K$. The projections to $\mathbb{A}^1$ are not finite, however, missing the point at ∞ above the origin. The same phenomenon can occur for an arbitrary irreducible closed subscheme curve $C \subset \mathcal{M}_K$ because $O_L \otimes \mathcal{M}_K \to \operatorname{Spec} O_L[B^{-1}]$ is not proper.

(2) Consider $C = \operatorname{Spec} \mathbb{Z}[T]/(f(T)) \subseteq \mathbb{A}^1_{\mathbb{Z}}$ with f monic. Then $C \to \operatorname{Spec} \mathbb{Z}$ is finite, but might be ramified. The same phenomenon can occur for an arbitrary curve $C \subset \mathcal{M}_K$.

Our proof of the finiteness in Thm. 3.5 makes use of the theory of Néron models. A more elementary argument for elliptic curves can be found in [12, Ex. VII.5.3].

Definition 3.7 ([1, Def. 1.2.1])**.** Let S be a connected Dedekind scheme with function field K and let A_K/K be an abelian variety. A Néron model of A_K is a smooth, separated, finite type scheme A/S together with an isomorphism $\operatorname{Spec} K \times_S A \cong A_K$ that has the following universal property: For every smooth S-scheme $X \to S$ and every generic map $u_K : \operatorname{Spec} K \times_S X \to A_K$, there is a unique extension to a map $u : X \to A$.

A Néron model is uniquely determined (up to unique isomorphism) by its universal property. Moreover, any Néron model is itself a group scheme, again by the universal property.

Theorem 3.8 ([1, Thm. 1.4.3])**.** *The Néron model always exists.*

Moreover, every abelian variety has potentially semi-abelian reduction in the following sense.

Theorem 3.9 ([1, Thm. 7.4.1])**.** *Let R be a DVR with fraction field K and A_K/K an abelian variety. Then there exists a finite extension $K \subseteq K'$ with the following property. Write $R' = \overline{R}^{K'}$ for the integral closure of R in K'. The Néron model A'/R' is such that for every maximal ideal $\mathfrak{m}'$ of $\operatorname{Spec} R'$,[4] say $k' = R'/\mathfrak{m}'$, A there exists an exact sequence*

$$1 \longrightarrow \mathbb{G}^t_{m,k'} \longrightarrow (k' \otimes_{R'} A')^\circ \longrightarrow B \longrightarrow 0 \tag{3.3}$$

where B/k' is an abelian variety. Here, $(k' \otimes_{R'} A')^\circ$ denotes the connected component of the identity element.

[4]Here R' is a semi-local PID. If R is complete, it is a DVR.

In this situation, all endomorphisms $\mathrm{End}(A_K)$ extend to A' by definition of the Néron model. Also, every endomorphism of A' preserves $(k' \otimes_{R'} A')^\circ$. Moreover, $\mathrm{Hom}(\mathbb{G}_{m,k'}, B) = 0$ because B is proper and $\mathbb{G}_m$ affine. Thus we obtain an action of $\mathrm{End}(A_K)$ on the kernel $\mathbb{G}^t_{m,k'}$ in (3.3). But we know $\mathrm{End}(\mathbb{G}_{m,k'}) = \mathbb{Z}$, so

$$\mathrm{End}(\mathbb{G}^t_{m,k'}) = M_t(\mathbb{Z}).$$

Thus if A_K admits complex multiplication in the sense that there exists a field extension $L/\mathbb{Q}$ with $[L:\mathbb{Q}] = 2\dim A_K$ and an embedding $O \to \mathrm{End}(A_K)$ for some order $O \subseteq O_L \subset L$, then $t = 0$ because there are no ring maps $O \to M_t(\mathbb{Z})$ for $1 \leq t \leq \dim A_K$. It follows that $(k' \otimes_{R'} A')^\circ = B$ is an abelian variety. In that situation, the next theorem applies.

Theorem 3.10 ([1, Thm. 7.4.5])**.** *Assume that R is a DVR with field of fractions K and residue field k. Assume that the Néron model A/R of an abelian variety A_K/K has connected component $(k \otimes_R A)^\circ$ an abelian variety. Then $k \otimes_R A$ itself is connected, i.e. A/R is an abelian scheme.*

Finiteness in Thm. 3.5. (1) First we argue that $\mathcal{C}_K \to \mathrm{Spec}\, O_L[B^{-1}]$ is quasi-finite. Let for this $V \subseteq \mathcal{M}_K$ be a vertical curve, i.e. V lies above some $\mathfrak{p} \in \mathrm{Spec}\, O_L[B^{-1}]$. Denote by E_V/V the universal elliptic curve. Its fiber E_η over the generic point $\eta \in V$ is ordinary, so for every finite extension $K/\kappa(\eta)$, the ring $\mathrm{End}^0(K \otimes_{\kappa(\eta)} E_\eta)$ is at most quadratic over $\mathbb{Q}$. Denote by V_K the normalization of V in K. By the Weil extension theorem and rigidity,

$$\mathrm{End}(K \otimes_{\kappa(\eta)} E_\eta) \subseteq \mathrm{End}(V_K \times_V E_V) \subseteq \mathrm{End}(\mathrm{Spec}\, \kappa(x) \times_V E_V)$$

for every closed point $x \in V_K$. But there always are supersingular and ordinary points x and we know that a quadratic extension can only act on a supersingular (resp. ordinary) elliptic curve in characteristic p if it is non-split (resp. split) at p. This shows that $\mathrm{End}(K \otimes_{\kappa(\eta)} E_\eta) = \mathbb{Z}$, so $\mathcal{C}_K$ cannot map onto a vertical curve in $\mathcal{M}_K$, proving the claimed quasi-finiteness.

(2) Now we verify the valuative criterion of properness for $\mathcal{C}_K \to \mathrm{Spec}\, O_L[B^{-1}]$. Let R be a DVR with field of fractions F and $(E_F, \iota, \bar{\eta}) \in \mathcal{C}_K(F)$. By Thm. 3.3, there exists a finite extension F'/F such that $F' \otimes_F E$ has semi-abelian reduction. Since it also has CM by L, it has to have an elliptic curve extension E'/R' by Thm. 3.10. The $O_L[B^{-1}]$-action ι extends to E' by the Weil extension theorem, the level structure by the valuative criterion of properness for the torsion $E'[B^m]$. The Kottwitz condition (3.1) can be checked generically over the DVR R'. Thus we obtain a tuple $(E', \iota, \bar{\eta}) \in \mathcal{C}_K(R')$. This is actually sufficient: Writing $\mathcal{M}_K = \mathrm{Spec}\, A$, we are given a ring homomorphism $A \to F$ such that the composition $A \to F \to F'$ has image in R'. Then the image lies in R, concluding the proof of the properness of $\mathcal{C}_K \to \mathrm{Spec}\, O_L[B^{-1}]$. □

Remark 3.11. Argument (1) in the above proof can be circumvented. Namely, knowing the properness from (2), the fact that $\mathcal{M}_K$ is affine implies that the image of $\mathcal{C}_K \to \mathcal{M}_K$ is finite over $\mathrm{Spec}\, O_L[B^{-1}]$. (The image is proper and affine, hence finite.) But $\mathcal{C}_K \to \mathcal{M}_K$ is unramified by Cor. 3.4, so $\mathcal{C}_K \to \mathrm{Spec}\, O_L[B^{-1}]$ itself is finite. Argument (1) in the above proof however carries over to other situations such as quaternionic Shimura curves, which might by proper themselves.

3.5. **Étaleness of $\mathcal{C}_K$.** Let $V(I) = S \hookrightarrow S'$ be a square-zero thickening, meaning $I^2 = 0$.

Theorem 3.12. *Assume that S is affine, let A/S be an abelian variety. There exists an abelian variety A'/S' such that $S \times_{S'} A' \cong A$.*

In general, for a smooth scheme X/S, there is an obstruction class in $H^2(X, I \otimes_{\mathcal{O}_S} T_{X/S})$ (cohomology of the tangent bundle) that determines whether or not X may be deformed to S'. Curves, for example, may always be deformed because $H^2(X, F) = 0$ for any

coherent sheaf F, but this does not carry over to higher-dimensional X/S. The key input for Thm. 3.12 is that the group law on A forces this obstruction to vanish. One may then show that the group law on A extends automatically to any deformation of A as variety. The isomorphism classes of deformations of A in turn are in bijection with the set $H^1(X, I \otimes_{\mathcal{O}_S} T_{X/S})$. All this is nicely explained in a blog post of A. Matthew. We now explain a theory that is more specific to abelian varieties, so-called Grothendieck–Messing deformation theory, cf. [8].

We assume from now on that $p \in \mathcal{O}_S$ is nilpotent, say $p^N = 0$. Consider the exact sequence

$$0 \longrightarrow A[p^N] \xrightarrow{p^N} A \longrightarrow A \longrightarrow 0.$$

Let E/S be a vector bundle, viewed as commutative group scheme, and apply $\mathrm{Hom}(-, E)$ to the sequence. Observe that $\mathrm{Hom}(A, E) = 0$ because of the properness of A, so we obtain an exact sequence

$$0 \longrightarrow \mathrm{Hom}(A[p^N], E) \longrightarrow \mathrm{Ext}^1(A, E) \xrightarrow{p^N} \mathrm{Ext}^1(A, E).$$

Using that $p^N E = 0$ and that $\mathrm{Ext}^1(-,-)$ is biadditive, the rightmost map vanishes and thus, naturally in A and E,

$$\mathrm{Hom}(A[p^N], E) = \mathrm{Ext}^1(A, E).$$

In general, if G/S is a finite, locally free, commutative group scheme, one may consider the functor $F \mapsto \mathrm{Hom}(G, F)$ on quasi-coherent $\mathcal{O}_S$-modules F. It is representable by $\omega_{G^*} = e^*\Omega^1_{G^*/S}$, where G^* is the Cartier dual of G. We take this statement on faith and refer to [8, §4] for more details.

Definition 3.13. The universal element in

$$\mathrm{Hom}(A[p^N], \omega_{A^*}) = \mathrm{Ext}^1(A, \omega_{A^*})$$

is called the universal vector extension of A, we denote it by $\widetilde{A}$,

$$0 \longrightarrow \omega_{A^*} \longrightarrow \widetilde{A} \longrightarrow A \longrightarrow 0. \tag{3.4}$$

The following is the main theorem of Grothendieck–Messing theory.

Theorem 3.14 ([8, Thm. IV.2.2])**.** *Let $S \to S'$ be a square-zero thickening.*[5] *Then there is a canonical deformation $\widetilde{A}(S')$ of the group scheme $\widetilde{A}$ to S'.*

The idea here is the following. First assume S affine. By Thm. 3.12, we find a deformation A' of A to S' and may take $\widetilde{A}(S') := \widetilde{A'}$. Then one shows that this is canonically independent of the choice of A' and in particular glues to a group scheme $\widetilde{A}(S')$. More generally, the cited [8, Thm. IV.2.2] provides for any homomorphism of abelian schemes $u : A \to B$ a canonical lifting $\widetilde{u} : \widetilde{A}(S') \to \widetilde{B}(S')$.

Definition 3.15. (1) The Grothendieck–Messing crystal of A, evaluated at S', is defined as the Lie algebra $D_A(S') := \mathrm{Lie}\,\widetilde{A}(S')$. It is a vector bundle of rank $2 \dim A$ over S'.

(2) The subsheaf $\omega_{A^*} \subset D_A(S)$ that comes from the universal extension (3.4) is called the Hodge filtration of A. It is a sub-vector bundle of rank g with the property that also the quotient $\mathrm{Lie}(A) = D_A(S)/\omega_{A^*}$ is locally free of rank g.

[5] The theory works more generally for divided power thickening.

Theorem 3.16. *Let $S \to S'$ be a square-zero thickening.*

(1) There is a bijection of deformations of A to S' and deformations of the Hodge filtration $\omega_{A^*} \subset D_A(S)$,

$$\begin{aligned} \left\{\text{Deformations } A'/S' \text{ of } A\right\} &\xrightarrow{\cong} \begin{Bmatrix} F' \subseteq D_A(S') \text{ such that } D_A(S')/F' \\ \text{is locally free and } \mathcal{O}_S \otimes_{\mathcal{O}_{S'}} F = \omega_{A^*} \end{Bmatrix} \\ A' &\longmapsto \omega_{A',*} \\ \widetilde{A}(S')/F' &\longmapsto\!\shortmid\ F'. \end{aligned} \tag{3.5}$$

(2) Let A', B' be abelian varieties over S' and let $u : S \times_{S'} A \to S \times_{S'} B$ be a homomorphism over S. Then u lifts to a homomorphism $u' : A' \to B'$ if and only if $D_u(S') : D_A(S') \to D_B(S')$ satisfies $D_u(\omega_{A',*}) \subseteq \omega_{B',*}$.

Recall that there is at most one u' in part (2) by rigidity. We deduce an interesting observation.

Corollary 3.17. *Assume $S \to S'$ is a nilpotent thickening, say $S = V(I)$ and $I^N = 0$. Assume that $p^m \in I$. Then, for any two abelian varieties A', B' over S',*

$$p^{m(N-1)} \operatorname{Hom}(S \times_{S'} A,\ S \times_{S'} B) \subseteq \operatorname{Hom}(A', B') \subseteq \operatorname{Hom}(A, B).$$

Here $A = S \times_{S'} A'$ and $B = S \times_{S'} B'$.

Proof. We need to show the inclusion on the left hand side. The chain $I \supseteq I^2 \supseteq \dots$ defines successive square-zero thickenings

$$S \subseteq V(I^2) \subseteq V(I^3) \subseteq \cdots \subseteq V(I^{N-1}) \subseteq S'.$$

By induction, we need to show that $u \in \operatorname{Hom}(V(I^i) \times_{S'} A',\ V(I^i) \times_{S'} B')$ implies that $p^m u \in \operatorname{Hom}(V(I^{i+1}) \times_{S'} A', V(I^{i+1}) \times_{S'} B')$. By Thm. 3.16, this holds if and only if the following composition vanishes,

$$\omega_{V(I^{i+1}) \times A',*} \longrightarrow D_{A'}(V(I^{i+1})) \xrightarrow{p^m D_u} D_{B'}(V(I^{i+1})) \longrightarrow D_{B'}(V(I^{i+1}))/\omega_{V(I^{i+1}) \times B',*}.$$

But the analogous composition for u vanishes modulo I^i and p^m lies in I, so that statement is clear. □

We warn the reader that Thm. 3.16 really has to be applied step-by-step. For example, even if $p\mathcal{O}_{S'} = 0$, it is not necessarily the case that $p \operatorname{Hom}(A, B) \subseteq \operatorname{Hom}(A', B)$.

Proof of the Étaleness in Thm. 3.5. We are now ready to show the étaleness of $\mathcal{C}_K \to \operatorname{Spec} O_L[B^{-1}]$. This we may do prime-by-prime, so let us fix some $p \nmid B$. Let $S \to S'$ be a square-zero thickening of $O_L[B^{-1}]$-schemes with $p \in \mathcal{O}_S$ locally nilpotent and $(E, \iota, \bar{\eta}) \in \mathcal{C}_K(S)$. We need to see that there is a unique deformation of this triple to S'. Giving $\bar{\eta}$ is an étale extra datum for (E, ι), so it is sufficient to deform (E, ι) (detail omitted). Let D be the Grothendieck–Messing crystal of E and

$$0 \longrightarrow \omega \longrightarrow D(S) \longrightarrow \operatorname{Lie}(E) \longrightarrow 0 \tag{3.6}$$

the Hodge filtration. All terms here have an additional $\mathcal{O}_S$-linear $O_L[B^{-1}]$-action. The evaluation $D(S')$ of the crystal on S' has an $\mathcal{O}_{S'}$-linear $O_L[B^{-1}]$-action.

Case p is unramified in L. There is then an isomorphism

$$O_L[B^{-1}] \otimes_{\mathbb{Z}} O_{L,p} \cong \mathbb{Z}_p \times \mathbb{Z}_p.$$

Because S' is an $O_L[B^{-1}]$-scheme and $p \in \mathcal{O}_{S'}$ locally nilpotent, this gives an isomorphism

$$O_L[B^{-1}] \otimes_{\mathbb{Z}} \mathcal{O}_{S'} \cong \mathcal{O}_{S'} \times \mathcal{O}_{S'} \tag{3.7}$$

which provides gradings $\omega = \omega_0 \oplus \omega_1$ and $D(S') = D'_0 \oplus D'_1$. (These are the two eigenspaces with eigenvalues $\zeta, \bar{\zeta}$ for a generator $O_L = \mathbb{Z}[\zeta]$.) The crucial observation now is that D'_0 and D'_1 are both line bundles, instead of (locally) one being trivial and the other rank 2. Namely we know that the Rosati involution acts as conjugation on $O_L[B^{-1}] \subseteq \mathrm{End}(E)$, so ω and $\mathrm{Lie}(E)$ have conjugate eigenvalue. The Kottwitz condition (3.1) now forces $D_0 \cong \mathrm{Lie}\, E$. Then ω and any $O_L[B^{-1}]$-stable lift $\omega' \subset D(S')$ are uniquely (!) determined as $\omega = D_1$ and $\omega' = D'_1$. It follows with Thm. 3.16 that there is a unique deformation of (E, ι) to S'.

Case p ramifies in L. Now the above eigenvalue argument breaks down. We claim that, still, $D(S')$ is free of rank 1 over $O_L[B^{-1}] \otimes_{\mathbb{Z}} \mathcal{O}_{S'}$. By Nakayama, this may be shown pointwise. So take $S = \mathrm{Spec}\, k$ and $S' = \mathrm{Spec}\, W(k)/p^2$. Then $D(S')$ is defined because $W(k)/p^2 \twoheadrightarrow k$ has square-zero kernel $pW(k)/p^2$. It is a module of length 4 over $W(k)/p^2$. Let π denote a uniformizer of O_L over p. Then π acts nilpotently on $D(S')$ and $\pi^2 D(S') = pD(S')$ has length 2. Thus $\ker(\pi)$ has length 1 and hence $\pi \neq 0 \bmod p$.

Now back to the case of general $S \subseteq S'$. By the Kottwitz condition (3.1), the quotient $D(S) \to \mathrm{Lie}\, E$ factors through

$$D(S) \twoheadrightarrow Q := \mathcal{O}_S \otimes_{O_L[B^{-1}] \otimes \mathcal{O}_S} D(S).$$

The map $O_L \otimes_{\mathbb{Z}} \mathcal{O}_S \to \mathcal{O}_S$ here comes from the structure map $S \to \mathrm{Spec}\, O_L$. The freeness of $D(S)$ implies that Q is a line bundle. Then $Q \twoheadrightarrow \mathrm{Lie}\, E$ has to be an isomorphism. The same argument also shows that there is a unique lift of ω to $\omega' \subseteq D(S')$ such that the $O_L[B^{-1}]$-action on $D(S')/\omega'$ satisfies the Kottwitz condition, namely

$$\omega' = \ker \left[D(S') \twoheadrightarrow \mathcal{O}_{S'} \otimes_{O_L[B^{-1}] \otimes \mathcal{O}_{S'}} D(S') \right],$$

which proves the étaleness also over ramified p. □

The picture for $\mathcal{C}_K$ is thus the following. Write $\mathrm{Spec}\, L \times_{\mathrm{Spec}\, O_L} \mathcal{C}_K = \coprod_{i \in I} \mathrm{Spec}\, H_i$ as a disjoint union of spectra of field extensions H_i/L. Then each H_i is unramified over L at primes $p \nmid B$ and

$$\mathcal{C}_K = \coprod_{i \in I} \mathrm{Spec}\, O_{H_i}[B^{-1}].$$

4. Canonical Liftings

Cor. 3.17 above makes a general, but coarse, statement about endomorphisms of deformations abelian varieties. The aim of this section is to prove a very precise result concerning deformations of CM elliptic curves. This actually computes the intersection numbers that occur in the Arithmetic Fundamental Lemma, Thm. 0.1, which we will see later.

4.1. **The setting.** Let $p \nmid B$ be a prime that is unramified in L.[6] Let $\mathfrak{p} \in \mathrm{Spec}\, O_L[B^{-1}]$ lie above p, put $\mathbb{F} = \overline{\mathbb{F}_{\mathfrak{p}}}$ and fix a point (E, ι). There is a unique mixed characteristic DVR with uniformizer p and residue field $\mathbb{F}$, namely the Witt vectors $W = W(\mathbb{F})$. Another way to obtain this ring is to consider the maximal unramified extension $\mathbb{Z}^{\mathrm{ur}} = \bigcup_{p \nmid n} \mathbb{Z}_p[\zeta_n]$ of $\mathbb{Z}_p$. Then $W = (\mathbb{Z}^{\mathrm{ur}})^{\wedge}_p$ coincides with its p-adic completion. There is a unique map $O_L \to W$ that reduces to

$$O_L/p \to \mathbb{F}_{\mathfrak{p}} \to \mathbb{F}.$$

Let (E_1, ι) be an elliptic curve over $\mathbb{F}$ together with an action $\iota : O_L[B^{-1}] \to \mathrm{End}(E)[B^{-1}]$ that satisfies the Kottwitz condition (3.1).

[6] This assumption is for simplicity only and excludes only finitely many primes.

Theorem 4.1. *There is a unique such pair (E, ι) over W with*

$$W/p \otimes_W (E, \iota) \cong (E_1, \iota).$$

The pair (E, ι) is called the canonical lifting of (E, ι).

Proof. Choose some small level K such that $\mathcal{C}_K$ is unramified and pick a K-level structurer $\bar{\eta}$ for (E_1, ι). (This exists because $\mathbb{F}$ is algebraically closed.) The étaleness in Thm. 3.5 provides unique deformations

$$(E_n, \iota, \bar{\eta}) : \operatorname{Spec} W/p^n \longrightarrow \mathcal{C}_K.$$

Writing $\mathcal{C}_K = \operatorname{Spec} A$ for some ring A, these correspond to a family of compatible O_L-algebra maps $A \to W/p^n$, which is the same as a ring map $A \to W$. In other words, there is a unique triple $(E, \iota, \bar{\eta}) \in \mathcal{C}_K(W)$ such that

$$(E_n, \iota, \bar{\eta}) \cong W/p^n \otimes_W (E, \iota, \bar{\eta}).$$

Given any other deformation (E', ι) of (E_1, ι), the chosen level structure $\bar{\eta}$ deforms uniquely showing $(E', \iota) \cong (E, \iota)$. □

Remark 4.2. The argument around (3.7) already showed the existence of a unique formal deformation $(\mathcal{E}, \iota)$ over the formal spectrum $\operatorname{Spf} W$. We picked K and argued with $\mathcal{C}_K$ in the above proof to argue that $(\mathcal{E}, \iota)$ is the p-adic completion of a pair (E, ι) over $\operatorname{Spec} W$.

Let (E, ι) be the canonical lifting of (E_1, ι). Put

$$(E_n, \iota) := W/p^n \otimes_W (E, \iota), \quad H_n := \operatorname{End}(E_n).$$

These rings form a descending chain

$$H_1 \supseteq H_2 \supseteq \ldots \supseteq H_\infty := \bigcap_{n \geq 1} H_n = \operatorname{End}(E).$$

We know that elliptic curves in characteristic 0 have endomorphism ring at most a quadratic extension, so $H_\infty \subset L$ is some order. By the existence of ι, this order is maximal away from B, i.e.

$$\operatorname{End}(E)[B^{-1}] = O_L[B^{-1}].$$

In case $p = \mathfrak{p}\bar{\mathfrak{p}}$ is split, the special fiber E_1 is ordinary and also has a quadratic endomorphism ring. By Cor. (3.17),

$$H_1[p^{-1}] = H_\infty[p^{-1}],$$

so in fact $H_1 = H_\infty$ because both orders are maximal at p. So assume from now on that $\mathfrak{p} = pO_L$ is inert. Then E_1 is supersingular and H_1 a maximal order O_D in a quaternion algebra $D/\mathbb{Q}$ that ramifies at $\{p, \infty\}$. This leaves us with the interesting question of what the endomorphism rings H_n are. The answer is provided by the following classical theorem of Gross.

Theorem 4.3 (Gross)**.** *The endomorphism ring $H_n = \operatorname{End}(W/p^n \otimes_W E)$ equals $H_\infty + p^{n-1}H_1$.*

This section is devoted to its proof.

4.2. **Divided powers.** The reference is [8, Chapter III]. We will just consider definitions and use results as black boxes.

The motivation is as follows. Assume R is an $\mathbb{Q}$-algebra and $I \subseteq R$ a nilpotent ideal or nil ideal.[7] Then exponential and logarithm provide an isomorphism

$$\begin{aligned} \exp : (I,+) &\xrightarrow{\cong} (1+I)^\times \\ x &\longmapsto \exp(x) = \sum_{i=0}^{\infty} \frac{x^n}{n!}. \end{aligned}$$

The occurring sum is finite by the nilpotency condition. This sometimes also works in characteristic p. For example, if $I^2 = 0$, then without any further assumptions on the ring R,

$$\begin{aligned} \text{“}\exp\text{“} : (I,+) &\xrightarrow{\cong} (1+I)^\times \\ x &\longmapsto 1+x. \end{aligned}$$

Another well-known example is, for $p > 2$,

$$\begin{aligned} \text{“}\exp\text{“} : (pW/p^nW,+) &\xrightarrow{\cong} (1+pW/p^nW)^\times \\ x &\longmapsto \text{“}\exp\text{“}(x) := \sum_{i=0}^{\infty} \frac{\widetilde{x}^n}{n!} \mod p^nW, \quad \widetilde{x} \in W \text{ lift of } x. \end{aligned}$$

In this last example, one has essentially provided an additional datum

$$\forall x \in I = pW/p^nW, \quad \gamma_n(x) := [\widetilde{x}^n/n! \mod p^nW] \in I$$

that allows to define the exponential. The notion of divided powers axiomatizes this concept.

Definition 4.4. Let R be a ring and $I \subseteq R$ an ideal. Divided powers on I are the datum of a series of maps $\gamma_n : I \to I,\ n \geq 1$ that satisfies

(1) $\gamma_1(x) = x$, we also put $\gamma_0(x) = 1$
(2) $\gamma_n(\lambda x) = \lambda^n x, \quad \lambda \in R,\ x \in I$
(3) $\gamma_n(x) \cdot \gamma_m(x) = \frac{(m+n)!}{m!n!}\gamma_{m+n}(x)$
(4) $\gamma_n(x+y) = \gamma_n(x) + \sum_{i=1}^{n-1} \gamma_{n-i}(x)\gamma_i(y) + \gamma_n(y)$
(5) $\gamma_m(\gamma_n(x)) = \frac{(mn)!}{(n!)^m m!}\gamma_{mn}(x)$.

Divided powers are called nilpotent if there is an $N \geq 1$ such that

$$\gamma_{n_1}(x_1) \cdots \gamma_{n_r}(x_r) = 0, \quad \forall r,\ n_1 + \ldots + n_r \geq N.$$

The third axiom provides $\gamma_1(x)\gamma_{n-1}(x) = n\gamma_n(x)$, so inductively $n!\gamma_n(x) = x$. In particular, if R is torsion free as $\mathbb{Z}$-module, then there is at most one choice of divided powers on I, namely $\gamma_n(x) = x/n!$. It always exists if R is a $\mathbb{Q}$-algebra.

Example 4.5. Let R be a DVR of mixed characteristic $(p,0)$ and ramification index e over $\mathbb{Z}_p$. This means that $p = u\pi^e$ for a uniformizer $\pi \in R$ and a unit $u \in R^\times$. The ideal (π^r) has at most one divided power structure because R is torsion free. It exists if and only if the fractions $\gamma_n(x) = x^n/n!$ lie in (π^r) itself. One computes

$$v_\pi(n!) = ev_p(n!) = e(\lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \ldots) \geq (n+1)r \quad \forall n \geq 1$$

if and only if $r \geq e/(p-1)$. The resulting divided powers are nilpotent if strict inequality $r > e/(p-1)$ holds. For example, pR always has divided powers which are topologically nilpotent if $p > 2$.

[7] Meaning that each $x \in I$ is nilpotent, but I itself need not be.

We note the following lemma to wrap up the current discussion.

Lemma 4.6 ([8, Def. III.1.5])**.** *Let R be a ring and I an ideal with nilpotent divided powers $(\gamma_n)_{n\geq 1}$. Then exponential and logarithm define mutually inverse isomorphisms $(I,+) \cong (1+I)^\times$,*

$$\exp(x) := \sum_{n=0}^{\infty} \gamma_n(x)$$

$$\log(1+x) := \sum_{n=1}^{\infty} (-1)^{n-1}(n-1)!\,\gamma_n(x).$$

4.3. **Grothendieck–Messing revisited.** Theorems (3.14) and (3.16) hold more generally for divided power thickenings. Let R be a ring in which p is nilpotent, $I \subseteq R$ a nilpotent ideal and $(\gamma_n)_{n\geq 1}$ nilpotent divided powers for I. Put $S = \operatorname{Spec} R/I$ and $S' = \operatorname{Spec} R$.

(1) Let A be an abelian variety over R/I. Its universal vector extension $\widetilde{A}$ deforms canonically to a smooth group scheme $\widetilde{A}(S')$ over S'. Taking its Lie algebra, we obtain a canonical deformation $D_A(S')$ of $D_A(S)$, defining the Grothendieck–Messing crystal of A.
(2) Deformations of A are in bijection with liftings of the Hodge filtration $\omega_{A^*} \subset D_A(S)$ to a locally direct summand $F \subset D_A(S')$.
(3) Given two abelian varieties $A', B'/S'$ and some $u \in \operatorname{Hom}(S \times_{S'} A', S \times_{S'} B')$, there is a canonical lifting $D_u(S') : D_{A'}(S') \to D_{B'}(S')$. Then u lies in $\operatorname{Hom}(A', B')$ if and only if $D_u(S')(\omega_{A',*}) \subseteq D_u(S')(\omega_{B',*})$.

We remark, that $\widetilde{A}(S')$ and $D_A(S')$ as well as the bijection in (2) depend on the given divided powers.

4.4. **Proof of Gross' Theorem.** We now prove Thm. 4.3. To simplify, we assume $p \neq 2$, even though the statement remains true for $p = 2$. Then the ideal pW has divided powers that are nilpotent modulo p^n for all $n \geq 1$. (This is called topologically nilpotent.) Passing to the limit, we may evaluate the Grothendieck–Messing crystal directly on W,

$$D := D_E(W) := \lim_{n\geq 1} D_E(W/p^n).$$

This is a free W-module of rank 2. The lifting property (3) in §4.3 provides a W-linear action $H_1 \to \operatorname{End}_W(D)$. (These objects only depend on the elliptic curve $E_1 = W/p \otimes_W E$.)

We next determine the structure of D as $W \otimes_{\mathbb{Z}} H_1$-module. Recall that H_1 is a maximal order in the quaternion division algebra over $\mathbb{Q}$ that is ramified precisely at p and ∞. Describing H_1 in general is complicated, just as with rings of integers in number fields. However, only the p-adic completion $H_{1,p}$ matters because

$$W \otimes_{\mathbb{Z}} H_1 = W \otimes_{\mathbb{Z}_p} H_{1,p}$$

and $H_{1,p}$ has the following simple description. There exists an element $\varpi \in H_{1,p}$ such that

$$H_{1,p} = O_{L,p}[\varpi], \quad \varpi^2 = p,\ \varpi a = \bar{a}\varpi\ \forall a \in O_{L,p}. \tag{4.1}$$

We know that the two eigenspaces $D = D_0 \oplus D_1$ of $O_{L,p}$ with respect to the two embeddings $O_{L,p} \to W$ are each 1-dimensional, see (3.7). Since ϖ Galois-commutes with $O_{L,p}$, cf. (4.1), it acts homogeneously on the eigenspace decomposition

$$\varpi : D_0 \longrightarrow D_1, \quad \varpi : D_1 \longrightarrow D_0.$$

Since $D_i \cong W$ as W-module and $\varpi^2 = p$, we find either

$$(\varpi D_0 = D_1,\ \varpi D_1 = pD_0) \ \text{ or } \ (\varpi D_0 = pD_1,\ \varpi D_1 = D_0).$$

But ϖ preserves the Hodge filtration D_1/pD_1 of $W/p \otimes_W E$ because H_1 "really" acts on E_1. Thus the first possibility has to occur. We summarize these findings as a lemma.

Lemma 4.7. *There exists a basis $D = W \oplus W$ such that the $H_{1,p}$-action $\mu : H_{1,p} \to M_2(W)$ takes the form*

$$\mu(a) = \begin{pmatrix} a & \\ & \bar{a} \end{pmatrix} \ \text{ for } a \in O_{L,p}, \quad \mu(\varpi) = \begin{pmatrix} & p \\ 1 & \end{pmatrix}.$$

Here, we viewed $O_{L,p}$ as a subset of $H_{1,p}$ via ι.

The Hodge filtration of the canonical lifting is D_1. It is stable under $O_{L,p}$ (by definition of the canonical lifting). Moreover,

$$(p^{n-1}\varpi)D_1 = p^n D_0,$$

so $H_{1,p} \cap \mathrm{Stab}(D_1/p^nD_1 \subset D/p^nD) = O_{L,p} + p^{n-1}H_1$. Grothendieck–Messing says that

$$\mathrm{End}(W/p^n \otimes_W E) = H_1 \cap \big(O_{L,p} + p^{n-1}H_{1,p}\big) = H_1 \cap O_{L,p} + H_1 \cap p^{n-1}H_{1,p}.$$

For the first intersection, $H_1 \cap O_{L,p} = H_\infty$. Namely every element of $H_1 \cap O_{L,p}$ preserves the Hodge filtration $D_1 \subseteq D$ and hence lifts to E. The second intersection is simply $p^{n-1}H_1$. So we obtain

$$\mathrm{End}(W/p^n \otimes_W E) = \mathrm{End}(E) + p^{n-1}\,\mathrm{End}(W/p \otimes_W E),$$

finishing the proof of Thm. 4.3. □

5. Hecke Correspondences

We are back to our standard setting: Let $\mathfrak{b} \in \mathbb{Z}$ denote the product of bad primes and $K \subset GL_2(\mathbb{Q}_\mathfrak{b})$ the level.

5.1. **Relative positions.** Let Λ_1, Λ_2 be two free $\mathbb{Z}$-modules of rank 2 and let $\varphi : \mathbb{Q}\otimes\Lambda_1 \to \mathbb{Q} \otimes \Lambda_2$ be an isomorphism. Whenever we choose $\mathbb{Z}$-bases for Λ_1, Λ_2, we obtain a matrix representation $\varphi \leftrightarrow g \in GL_2(\mathbb{Q})$. Since different bases differ by an element of $GL_2(\mathbb{Z})$, the double coset $GL_2(\mathbb{Z})gGL_2(\mathbb{Z})$ is an invariant of φ.

Definition 5.1. The double coset $GL_2(\mathbb{Z})gGL_2(\mathbb{Z})$ is called the relative position of Λ_1 and Λ_2 under φ.

The occurring double quotient is described by the elementary divisor theorem.

Theorem 5.2. *There is a disjoint union decomposition*

$$GL_2(\mathbb{Q}) = \coprod_{a,b\in\mathbb{Q}_{>0},\ v_p(a)\geq v_p(b)\forall p} GL_2(\mathbb{Z}) \begin{pmatrix} a & \\ & b \end{pmatrix} GL_2(\mathbb{Z}).$$

An analogous result holds for any principal ideal domain. Replacing lattices by elliptic curves, we arrive at the concept of relative position for quasi-isogenies. I immediately specialize to $\mathfrak{b}$-isomorphisms in the following sense.

Definition 5.3. A $\mathfrak{b}$-isomorphism of two elliptic curves A, B over some scheme S is an invertible element $\varphi \in \mathrm{Hom}(A, B)[\mathfrak{b}^{-1}]$. In other words $\deg(\varphi) \in \prod_{p|\mathfrak{b}} p^{\mathbb{Z}}$.

Let $S/\mathbb{Z}[\mathfrak{b}^{-1}]$ be any scheme, $(A, \bar\eta_A), (B, \bar\eta_B) \in M_K(S)$ and $\varphi : A \to B$ a $\mathfrak{b}$-isomorphism.

Definition 5.4. The relative position of φ is the double coset

$$\bar{\eta}_B^{-1}\varphi\bar{\eta}_A \in GL_2(\mathbb{Z}_\mathfrak{b})\backslash GL_2(\mathbb{Q}_\mathfrak{b})/GL_2(\mathbb{Z}_\mathfrak{b}).$$

Let $\mu \in GL_2(\mathbb{Z}_\mathfrak{b})\backslash GL_2(\mathbb{Q}_\mathfrak{b})/GL_2(\mathbb{Z}_\mathfrak{b})$ denote such a double coset in the following.

Example 5.5. (1) Let $(A, \bar{\eta})$ lie above $S = \operatorname{Spec} k$ with k algebraically closed. Pick any $\eta \in \bar{\eta}$ and any $g \in \mu$. Then

$$\mathrm{id}_A : (A, \eta K) \longrightarrow (A, \eta g K) \tag{5.1}$$

has relative position μ. Conversely, given any $\varphi : (A, \bar{\eta}_A) \to (B, \bar{\eta}_B)$ of relative position μ, first observe that φ defines an isomorphism $(A, \varphi^{-1}\bar{\eta}_B) \cong (B, \bar{\eta}_B)$, so without loss of generality $A = B$. This puts us in a situation

$$\gamma : (A, \bar{\eta}) \longrightarrow (A, \bar{\eta}').$$

Picking any $\eta \in \bar{\eta}$ and $\eta' \in \bar{\eta}'$, there is a unique $g \in GL_2(\mathbb{Q}_\mathfrak{b})$ such that $\eta' = \eta g$. Thus, γ is of the form (5.1).

(2) Assume $\mathfrak{b} = p \cdot \mathfrak{b}'$ with $p \nmid \mathfrak{b}'$. Assume further that $K = K_p \times K^p$ with $K^p \subset GL_2(\mathbb{Q}_{\mathfrak{b}'})$ and $K_p = GL_2(\mathbb{Z}_p)$. Then $M_K = M_{K^p}[p^{-1}]$ and we recover the Hecke operator T_p from last term if we set

$$\mu = K_p \begin{pmatrix} p & \\ & 1 \end{pmatrix} K_p \times K_{\mathfrak{b}'}.$$

Indeed, $\varphi : (A, \bar{\eta}_A) \to (B, \bar{\eta}_B)$ is of relative position μ if and only if φ preserves the $\mathfrak{b}'$-level structure and puts the Tate modules at p in relative position $\mathrm{diag}(1, p)$. The latter means it is an isogeny of degree p. More generally, if

$$\mu = K_p \begin{pmatrix} p^a & \\ & p^b \end{pmatrix} K_p \times K_{\mathfrak{b}'}$$

with $a, b \geq 0$, then instead φ is required to have $\ker(\varphi) \cong \mathbb{Z}/p^a \oplus \mathbb{Z}/p^b$ (étale locally).

(3) Keep $K_{\mathfrak{b}'}$ as above, but take $K_p = \ker(GL_2(\mathbb{Z}_p) \to GL_2(\mathbb{Z}/p^n))$. Then Prop. 2.10 allows to describe points of M_K as triples $(A, \bar{\eta}, \alpha)$, where $\bar{\eta}$ is a $K_{\mathfrak{b}'}$-level structure and $\alpha : (\mathbb{Z}/p^n)^{\oplus 2} \cong A[p^n]$ a level structure in the classical sense. Now take $\mu = gK_p$ with some $g \in GL_2(\mathbb{Z}_p)$. Since $K_p \subseteq GL_2(\mathbb{Z}_p)$ is normal, this right coset is simultaneously a left coset. Then for any $(A, \bar{\eta}, \alpha)$, there is a unique emanating isogeny of relative position $K_{\mathfrak{b}'} \times gK_p$ up to isomorphism, namely

$$\mathrm{id}_A : (A, \bar{\eta}, \alpha) \longrightarrow (A, \bar{\eta}, \alpha g).$$

5.2. **Hecke correspondences.**

Definition 5.6. Let $\mu \in K\backslash GL_2(\mathbb{Q}_\mathfrak{b})/K$ be a double coset. The Hecke operator $R(\mu)$ is the functor

$$R(\mu) = \left\{ (A, \bar{\eta}_A, B, \bar{\eta}, \varphi) \;\middle|\; \begin{array}{c} (A, \bar{\eta}_A), (B, \bar{\eta}_B) \in M_K \\ \varphi \in \mathrm{Hom}(A, B)[\mathfrak{b}^{-1}]^\times \\ \bar{\eta}_B^{-1}\varphi\bar{\eta}_A = \mu \end{array} \right\}.$$

Here, an isomorphism of quintuples

$$(A, \bar{\eta}_A, B, \bar{\eta}_B, \varphi) \cong (A', \bar{\eta}'_A, B', \bar{\eta}'_B, \varphi')$$

is a pair of isomorphisms $\varphi_A : (A, \bar{\eta}_A) \cong (A', \bar{\eta}'_A)$ and $\varphi_B : (B, \bar{\eta}_B) \cong (B', \bar{\eta}'_B)$ such that $\varphi' = \varphi_A \varphi \varphi_B^{-1}$.

In other words, $R(\mu)$ parametrizes isogenies of relative position μ.

Proposition 5.7. *Assume that M_K is representable. Then $R(\mu)$ is also representable. The two projection maps $p_1, p_2 : R(\mu) \to M_K$ are finite étale. In particular, $R(\mu)$ is smooth over $\mathbb{Z}[\mathfrak{b}^{-1}]$.*

Proof. Observe that $R(\mu) \cong R(\mathfrak{b}^n\mu)$, $\varphi \mapsto \mathfrak{b}^n\varphi$ and that this isomorphism commutes with both projections. In this way, we may assume $\mu \subset M_2(\mathbb{Z}_\mathfrak{b})$ in the following. Then all $\varphi \in R(\mu)$ are actual isogenies.

Assume M_K is representable, consider the universal pair $(E, \bar\eta)/M_K$. By Thm. 3.3, the Hom-functor

$$\underline{\mathrm{Hom}}(p_1^*E, p_2^*E) \to M_K \times_{\mathrm{Spec}\,\mathbb{Z}[\mathfrak{b}^{-1}]} M_K, \quad n \geq 0$$

is representable. Moreover, the relative position of an isogeny is locally constant in families, so $R(\mu)$ is an open and closed subscheme of H.

Our argument for finite étaleness extends Ex. 5.5 (1). First note that one may show the claimed properties after any fpqc base change $S' \to S = M_K$. We choose $S' \to S$ such that there exists a Tate module trivialization $\eta \in \bar\eta(S')$ of the pull back of the universal curve $S' \times_S E$. Now we expand Ex. 5.5: Assume

$$(T \times_S E, T \times_S \bar\eta, B, \bar\eta_B, \varphi) \in (S' \times_S R(\mu))(T).$$

Then φ defines an isomorphism $(T \times_S E, T \times_S \varphi^{-1}\bar\eta_B) \cong (B, \bar\eta_B)$, so we may assume $B = T \times_S E$. We have fixed a trivialization

$$\eta : \underline{\mathbb{Q}}_\mathfrak{b}^2 \xrightarrow{\cong} V_\mathfrak{b}(T \times_S E)$$

of the rational Tate module. This allows to write $\varphi^{-1}\bar\eta_B = \eta\bar g$ for a unique function $\bar g : T \to GL_2(\mathbb{Q}_\mathfrak{b})/K$. (The target here is discrete and $\bar g$ locally constant.) Since φ has relative position μ, this function takes values in μ/K. In this way, we have defined a map to the constant scheme μ/K,

$$S' \times_S R(\mu) \longrightarrow \coprod_{\mu/K} S'. \tag{5.2}$$

An inverse map is given by

$$[\bar g : T \to \mu/K] \longmapsto (T \times_S E, \bar\eta, T \times_S E, \eta g K, \mathrm{id}),$$

showing that (**??**) is an isomorphism. □

Example 5.8. For μ as Ex. 5.5 (2), the Hecke operator $R(\mu)$ agrees with $T_p[p^{-1}]$ from last term. For μ as in (3), $R(\mu)$ is the graph Γ_g of the automorphism defined by g.

6. CM Cycle Intersection I

This chapter forms the heart of the lecture. It brings together all objects defined so far in an interesting intersection problem[8] and develops a group-theoretic expression for the occurring intersection numbers.

[8]This is the intersection problem that occurred in §1 of course.

6.1. **Intersection numbers.** The following is our setting.

(1) $\mathfrak{b} \in \mathbb{Z}$ is the product of bad primes.
(2) $G = GL_{2,\mathbb{Q}}$, while $K \subset G(\mathbb{Q}_\mathfrak{b})$ denotes the level.
(3) $L/\mathbb{Q}$ is an imaginary-quadratic field with torus $T = L^\times$. Moreover, we fix an embedding $L \to M_2(\mathbb{Q})$, which allows to view $T \subset G$.
(4) We assume that all ramified primes of $L/\mathbb{Q}$ divide $\mathfrak{b}$. We work with schemes over $O_L[\mathfrak{b}^{-1}]$.
(5) $M_K \to \operatorname{Spec} O_L[\mathfrak{b}^{-1}]$ denotes the (base change to $O_L[\mathfrak{b}^{-1}]$) modular curve from §2. We assume K is small enough in order for M_K to be representable.
(6) $C_K \to M_K$ denotes the CM cycle from §3.
(7) $\mu \in K \subset GL_2(\mathbb{Q}_\mathfrak{b})/K$ is a double coset and
$$R(\mu) \longrightarrow M_K \times_{\operatorname{Spec} O_L[\mathfrak{b}^{-1}]} M_K$$
the Hecke correspondence from §5.

From a theory-building point of view, our interest lies with the intersection problem that arises by applying $R(\mu)$ to the cycle defined by C_K,
$$([C_K],\ p_{1,*}(R(\mu) \cdot p_2^*[C_K]))\,.$$
In our situation, this leads to the very concrete problem of analyzing the scheme
$$I(\mu) := R(\mu) \times_{M_K \times M_K} (C_K \times C_K)\,.$$
Two cases may occur.

(1) The intersection $I(\mu)$ is of the expected dimension 0. (This is "expected" because we are intersecting curves on a surface.) In this case, $I(\mu)$ is an artinian scheme and we define the intersection number
$$\operatorname{Int}(\mu) := \log|\mathcal{O}_{I(\mu)}| = \sum_{p \nmid \mathfrak{b}} \sum_{x \in \mathbb{F}_p \otimes_\mathbb{Z} I(\mu)} \ell_{\mathbb{Z}_p}(\mathcal{O}_{I(\mu),x}) \log(p).$$
This is the analogue of the length in the arithmetic setting. Namely the product formula reads
$$\prod_{p \leq \infty} |x|_p = 1$$
for every rational number $x \in \mathbb{Q}^\times$, motivating the multiplicative normalization.
(2) The intersection is degenerate in the sense that $\dim I(\mu) = 1$. To define $\operatorname{Int}(\mu)$ in this case requires to compactify the modular curve both vertically (generalized elliptic curves) and horizontally (Arakelov theory). This is of course necessary for a full proof of the Gross–Zagier formula, but lies beyond this course.

Recall Thm. 3.5, which states that $C_K \to \operatorname{Spec} O_L[\mathfrak{b}^{-1}]$ is finite étale. So degenerate intersection occurs if and only if the generic fiber $\operatorname{Spec} L \times I(\mu)$ is non-empty. From the point of view of this course, we would like to exclude this case.

6.2. **Regular Semi-Simple elments I.** The map $L \to M_2(\mathbb{Q})$ makes $\mathbb{Q}^2$ into a 1-dimensional L-vector space. Canonically,
$$\operatorname{End}_L(\mathbb{Q}^2) = L$$
as this holds for every 1-dimensional L-vector space. Pick a basis, say $\mathbb{Q}^2 = L \cdot u$. Then Galois conjugation with respect to this basis element, $\sigma(x \cdot u) := \bar{x} \cdot u$, defines an automorphism $\sigma \in GL_2(\mathbb{Q})$ that Galois commutes with L, meaning
$$\sigma x = \bar{x}\sigma \quad \text{for all } x \in L.$$

Every other Galois linear element of $M_2(\mathbb{Q})$ differs by an L-linear element from σ, and we obtain

$$M_2(\mathbb{Q}) = L \oplus L \cdot \sigma.$$

All terms may be viewed as affine varietes ($\mathbb{A}^2$ or $\mathbb{A}^4$) over $\mathbb{Q}$, from which we obtain a subgroup

$$N := T \sqcup T\sigma \subset G.$$

The group N agrees with the normalizer of T in G, i.e. $g \in N(S)$ if and only if $g(S \times T)g^{-1} = S \times T$.

Definition 6.1. The complement $G_{\mathrm{rs}} := G \setminus N$ is called the set of regular semi-simple elements.

There is also a group-theoretic characterization which will come up later, but the next result has us happy for now.

6.3. **Support of $I(\mu)$.**

Proposition 6.2. *Assume that $\mu \subset G_{\mathrm{rs}}(\mathbb{Q}_{\mathfrak{b}})$. Then $I(\mu)$ is artinian. In fact,* $\operatorname{Supp} I(\mu)$ *consists of supersingular points only.*

Proof. The intersection $I(\mu)$ is 1-dimensional if and only if $I(\mu)_L \neq \emptyset$. Let us assume that

$$(A, \eta_A : L_{\mathfrak{b}} \cong V_A, B, \eta_B : L_{\mathfrak{b}} \cong V_B, \varphi) \in (R(\mu) \times (C_K \times C_K))\,(\bar{L}).$$

Here, η_A and η_B denote L-linear representatives of the respective level structures. Now note that, because A and B lie in characteristic 0, their endomorphism rings agree with L. Thus, even though the definition of $R(\mu)$ has no relation with the CM cycle, φ is automatically L-linear or L-Galois-linear. Thus we find

$$\eta_B^{-1}\varphi\eta_A \in \mu \cap N(\mathbb{Q}_{\mathfrak{b}}),$$

showing that μ is not contained in regular semi-simple elements. (In fact, φ is L-linear because it induces an $\bar{L}$-linear map on Lie algebras and the Kottwitz condition ensures that the two maps from L to $\operatorname{End}(\operatorname{Lie} A) = \operatorname{End}(\operatorname{Lie} B) = \bar{L}$ agree.)

Now assume $\mu \subseteq G_{\mathrm{rs}}(\mathbb{Q}_{\mathfrak{b}})$ and that $(A, \eta_A, B, \eta_B, \varphi) \in (R(\mu) \times (C_K \times C_K))(\overline{\mathbb{F}_v})$ for some place $v \nmid \mathfrak{b}$ of L. Again, η_A and η_B are chosen L-linearly here. Write

$$\iota_A : O_L \to \operatorname{End}(A)[\mathfrak{b}^{-1}] \quad \text{resp.} \quad \iota_B : O_L \to \operatorname{End}(B)[\mathfrak{b}^{-1}]$$

for the two actions. The relative position of φ cannot be that of an L-linear or L-Galois-linear element, so φ cannot be L-(Galois-)linear. It follows that $\varphi^{-1}\iota_B(L)\varphi \neq \iota_A(L)$. Thus $\operatorname{End}^0(A)$ has to be of dimension > 2 and hence a division algebra, as was to be shown. □

Note that this implies $\mathbb{F}_v \otimes I(\mu) = \emptyset$ whenever v splits in O_L because all points on $I(\mu)$ have CM by L.

6.4. **Supersingular points of M_K.** In order to describe the points of $I(\mu)$, we first have to understand supersingular points on M_K.

Theorem 6.3. *Let A and B be supersingular elliptic curves over an algebraically closed field k of characteristic p. Then there exists an isogeny $\varphi : A \to B$.*

Remark 6.4. This theorem has two important generalizations. The first is Honda–Tate theory, which provides a classification of abelian varieties (up to isogeny) over finite fields. The second is the uniformization theorem for the basic locus of Shimura varieties, stating that the points in this locus form a single isogeny class.

Proof. The proof relies on lifting A and B to CM elliptic curves in characteristic 0, which is achieved by the following arguments.

We have seen in previous courses that every supersingular elliptic curve is defined over $\mathbb{F}_{p^2}$. So we may replace A and B by models over $\mathbb{F}_{p^2}$. Passing to some prime power $q = p^{2r}$, we may assume that $\mathrm{End}(A)$ and $\mathrm{End}(B)$ have rank 4. We know that in this case,

$$O_D \cong \mathrm{End}(A) \cong \mathrm{End}(B)$$

are isomorphic to a maximal order O_D in the quaternion division algebra $D/\mathbb{Q}$ that is non-split at $\{p, \infty\}$. Thus we find an imaginary quadratic extension $L/\mathbb{Q}$ that is inert at p, some $\mathfrak{b}$ with $p \nmid \mathfrak{b}$, and embeddings

$$\iota_A : O_L[\mathfrak{b}^{-1}] \to \mathrm{End}(A), \quad \iota_B : O_L[\mathfrak{b}^{-1}] \to \mathrm{End}(B).$$

We fix a map $O_L \to \mathbb{F}_q$. Then, possibly replacing ι_A and ι_B by their Galois conjugates, we may assume them to satisfy the Kottwitz condition. After replacing q by a power, we may also make an auxiliary choice of a small level group K, a map $L \to M_2(\mathbb{Q})$, and L-linear level structures η_A and η_B. In this way, we have constructed

$$(A, \iota_A, \eta_A),\ (B, \iota_B, \eta_B) \in C_K(\mathbb{F}_q).$$

The CM cycle C_K is finite étale over $O_L[\mathfrak{b}^{-1}]$, so there is a finite extension H/L with a map $O_H \to \mathbb{F}_q$ and liftings

$$(\widetilde{A}, \iota_A, \eta_A), (\widetilde{B}, \iota_B, \eta_B) \in C_K(O_H[\mathfrak{b}^{-1}]).$$

Now we may reap rewards: All elliptic curves with CM by the same field L in characteristic 0 are isogeneous, which may be checked over $\mathbb{C}$. Thus, after an extension H'/H, there exists an isogeny $H' \otimes \widetilde{A} \to H' \otimes \widetilde{B}$. By Weil extension/Néron property, it extends to an isogeny

$$O_{H'}[\mathfrak{b}^{-1}] \otimes \widetilde{A} \longrightarrow O_{H'}[\mathfrak{b}^{-1}] \otimes \widetilde{B}$$

and we win. □

Consider the units $D^\times$ as (4-dimensional, smooth, connected, affine) group scheme over $\mathrm{Spec}\,\mathbb{Q}$, it is defined as

$$D^\times(R) := (R \otimes_{\mathbb{Q}} D)^\times.$$

Then $D^\times(\mathbb{A}_f^p) \cong GL_2(\mathbb{A}_f^p)$ because D splits outside $\{p, \infty\}$. Let us again write

$$K^\circ := K \times GL_2(\widehat{\mathbb{Z}}^{\mathfrak{b}})$$

for the completed level subgroups. Any choice of isomorphism γ (of $\mathbb{Q}_{\mathfrak{b}}$-points) allows to consider the open compact subgroup $\gamma^{-1}(K^{\circ,p})$. There is a unique maximal order $O_{D,p}$ in the p-adic completion D_p, which allows to canonically plug in $O_{D,p}^\times$ at p to obtain double quotients of the form

$$D^\times \backslash D^\times(\mathbb{A}_f) / \gamma^{-1}(K^{\circ,p}) \times O_{D,p}^\times.$$

These are finite, which is a general property of adelic groups.

Proposition 6.5. *Consider M_K over $\mathbb{Z}[\mathfrak{b}^{-1}]$. The number of supersingular points in $M_K(\overline{\mathbb{F}}_p)$ is*

$$D^\times \backslash D^\times(\mathbb{A}_f) / \gamma^{-1}(K^{\circ,p}) \times O_{D,p}^\times,$$

where γ is any choice of isomorphism. This relies on some identifications. More naturally,[9] *let $A/\overline{\mathbb{F}}_p$ be any supersingular elliptic curves. Then $M_K^{\mathrm{ss}}(\overline{\mathbb{F}}_p)$ is in bijection with*

$$\mathrm{Aut}^0(A) \backslash \left(\mathrm{Isom}((\mathbb{A}_f^p)^2, V^p(A)) / (K^{\circ,p}) \times D_p^\times / O_{D,p}^\times \right).$$

[9] But also more clumsily...

Proof. The result looks more complicated than it really is. The idea is simply that, since all supersingular elliptic curves are isogeneous by Thm. 6.3, we first enumerate isoegenies to a fixed elliptic curve A and then quotient out self-quasi-isogenies of A. In other words, we already know

$$M_K^{\mathrm{ss}}(\overline{\mathbb{F}}_p) = \mathrm{Aut}^0(A)\backslash\{(B,\bar\eta,\varphi : B \to A)\},$$

where $(B,\bar\eta) \in M_K(\overline{\mathbb{F}}_p)$ and where φ is any quasi-isogeny. The statement is just about giving a more concrete definition of the right hand side.

Pick an auxiliary $\xi : (\mathbb{A}_f^p)^2 \cong V^p(A)$. The adelic points $D^\times(\mathbb{A}_f^p)$, where $D = \mathrm{End}^0(A)$, act naturally on the right. The choice ξ provides an isomorphism

$$\gamma = D^\times(\mathbb{A}_f^p) \cong GL_2(\mathbb{A}_f^p),\ g \mapsto \xi^{-1}g\xi. \tag{6.1}$$

Given some $(B,\bar\eta,\varphi)$, we now construct

(1) The composition $x_{\mathfrak{b}} = \xi^{-1}\varphi\eta \in GL_2(\mathbb{Q}_{\mathfrak{b}})/K$.
(2) The lattice $x^{p\mathfrak{b}} = \xi^{-1}\varphi T^{p\mathfrak{b}}(B) \in GL_2(\mathbb{A}_f^{p\mathfrak{b}})/GL_2(\widehat{\mathbb{Z}}^{p\mathfrak{b}})$.
(3) The p-degree
$$x_p = v_p(\deg\varphi) \in \mathbb{Z} \cong D_p^\times/O_{D,p}^\times.$$

The isomorphism (6.1) allows to view $(x_{\mathfrak{b}}, x^{p\mathfrak{b}}, x_p) \in D^\times(\mathbb{A}_f)/\gamma^{-1}(K^{\circ,p}) \times O_{D,p}^\times$. We leave it to the reader to check that, conversely, such triples are in bijection with the previous triples $(B,\bar\eta,\varphi)$.

Any other choice of φ takes the form $g\varphi$ with $g \in \mathrm{Aut}^0(A)$, which induces the following transformation.

(1) The element $x_{\mathfrak{b}} = \xi^{-1}\varphi\eta$ changes to $\xi^{-1}g\varphi = \gamma(g)x_{\mathfrak{b}}$.
(2) The lattice $x^{p\mathfrak{b}} = \xi^{-1}\varphi T^{p\mathfrak{b}}(B)$ changes to $\gamma(g)x^{p\mathfrak{b}}$.
(3) The p-degree $x_p = v_p(\deg\varphi)$ changes to $v_p(g) + x_p$, which amounts to gx_p when viewed as element of $D_p^\times/O_{D,p}^\times$.

Applying γ^{-1}, we obtained a bijection

$$M_K^{\mathrm{ss}}(\overline{\mathbb{F}}_p) \cong D^\times\backslash D^\times(\mathbb{A}_f)/\gamma^{-1}(K^{\circ,p}) \times O_{D,p}^\times$$

as claimed. □

The above arguments involved level structures and the representability implicitly: Each point $x \in M_K^{\mathrm{ss}}(\overline{\mathbb{F}}_p)$ is a point and contributes 1. The following, beautiful and classical corollary explains how to extend this counting to the stack of elliptic curves itself.

Corollary 6.6. *Let p be a prime. Then*

$$\sum_{E \in \{\textit{supersing. } EC/\overline{\mathbb{F}}_p\}/\cong} \frac{1}{\mathrm{Aut}(E)} = \frac{p-1}{24}.$$

Proof. Pick $n \geq 3$ with $p \nmid n$. Let $O_D \subset D$ be a maximal order and put $K(n) = \ker(\widehat{O_D}^\times \to (O_D/nO_D)^\times)$. Then the bijection

$$\{\text{supersing. EC with level-}n\text{-structure}/\overline{\mathbb{F}}_p\}/\cong \overset{1:1}{\longleftrightarrow} D^\times\backslash D^\times(\mathbb{A}_f)/K(n)$$

from Prop. 6.5 is equivariant for the natural $GL_2(\mathbb{Z}/n\mathbb{Z})$-action on both sides. Thus, counting orbits weighted by orders of stabilizer groups, one obtains

$$\sum_{E \in \{\text{supersing. EC}/\overline{\mathbb{F}}_p\}/\cong} \frac{1}{\mathrm{Aut}(E)} = \mathrm{Vol}\left(D^\times\backslash D^\times(\mathbb{A}_f)/\widehat{O_D}^\times\right) = \frac{|\mathcal{C}\ell_D|}{|O_D^\times|}.$$

Here $\mathcal{C}\ell_D$ is the class group of D, defined as the quotient group of fractional ideals in D modulo principal ideals. Using elementary arguments, one may evaluate this right hand side as $(p-1)/24$. □

7. CM Cycle Intersection II

7.1. **Points of $C_K(\overline{\mathbb{F}}_p)$.** Let all notation be as in §6.1. Recall that last week we parametrized supersingular elliptic curve in characteristic p by considering quasi-isogenies from a fixed one. Let

(1) $C/\overline{\mathbb{F}}_p$ a fixed supersingular elliptic curve
(2) $\xi : (\mathbb{A}_f^p)^2 \xrightarrow{\cong} V^p(C)$ a choice of full level structure
(3) $D := \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(C)$ the endomorphism ring.

Define the set

$$R := \left\{ (A, \bar{\eta}_A, \phi_A) \;\middle|\; \begin{array}{c} (A, \bar{\eta}_A) \in M_K^{\mathrm{ss}}(\overline{\mathbb{F}}_p) \\ \phi_A : A \to C \text{ any quasi-isogeny} \end{array} \right\} / \cong .$$

Then

$$\begin{array}{rl} R \xrightarrow{\cong} & D(\mathbb{A}_f)^\times / K^{\circ,p} \times \widehat{O_D}^\times \\ (A, \bar{\eta}_A, \phi_A) \longmapsto & (\xi^{-1}\phi_A \eta_A, v_p(\deg(\phi_A))). \end{array}$$

Theorem 7.1 (Skolem–Noether)**.** *Let k be a field, L a simple k-algebra, and D a central simple k-algebra. Then all maps $L \to D$ are conjugate.*

Pick any L-action on C and make an L-linear choice for ξ. (This is meant with respect to the datum $L \to M_2(\mathbb{Q})$ from §6.1.) The Skolem–Noether Theorem applies and yields

Corollary 7.2. *For every point $(A, \iota_A, \bar{\eta}_A) \in C_K(\overline{\mathbb{F}}_p)$, there is an L-linear quasi-isogeny $\phi_A : A \to C$.*

Put

$$S := \left\{ (A, \bar{\eta}_A, \iota_A, \phi_A) \mid \;\middle|\; \begin{array}{c} (A, \iota_A, \bar{\eta}_A) \in C_K(\overline{\mathbb{F}}_p) \\ \phi_A : A \to C \text{ any } L\text{-linear quasi-isogeny} \end{array} \right\} / \cong .$$

Proposition 7.3. *There are bijections*

$$\begin{array}{rl} T \xrightarrow{\cong} & T(\mathbb{A}_f)/T(\mathbb{A}_f) \cap K^\circ \\ (A, \iota_A, \bar{\eta}_A, \phi_A) \longmapsto & (\xi^{-1}\phi_A \eta_A, v_p(\deg(\phi_A)). \end{array} \tag{7.1}$$

and

$$C_K(\overline{\mathbb{F}}_p) \xrightarrow{\cong} T(\mathbb{Q}) \backslash T(\mathbb{A}_f)/T(\mathbb{A}_f) \cap K^\circ. \tag{7.2}$$

7.2. **Points of $I(\mu)$.** Using the same method, we now describe $I(\mu)(\overline{\mathbb{F}}_p)$. Recall here that

$$I(\mu) = R(\mu) \times_{M_K \times M_K} (C_K \times C_K).$$

Consider

$$T := \left\{ (A, \bar{\eta}_A, \iota_A, \phi_A, B, \bar{\eta}_B, \iota_B, \phi_B, \varphi) \;\middle|\; \begin{array}{c} (A, \iota_A, \bar{\eta}_A), (B, \iota_B, \bar{\eta}_B) \in C_K(\overline{\mathbb{F}}_p) \\ \phi_A : A \to C \text{ and } \phi_B : B \to C \text{ are } L\text{-linear quasi-isogenies} \\ \varphi : A \to B \text{ is a quasi-isogeny of relative position } \mu \end{array} \right\} / \cong .$$

Given such a tuple, we may construct the following elements.

(1) $x_A := \xi^{-1}\phi_A \bar{\eta}_A$ and $x_B := \xi^{-1}\phi_B \bar{\eta}_B$ in $T(\mathbb{A}_f)/(T \cap K^\circ) \subset D(\mathbb{A}_f)^\times / (K^{\circ,p} \times \widehat{O_D}^\times)$.
(2) $\gamma := \phi_B \circ \varphi \circ \phi_A^{-1} \in D^\times$.

Observe the following identity, which simply comes from tracing through definitions:

$$\bar{\eta}_B^{-1}\varphi\bar{\eta}_A = (\xi^{-1}\phi_B\eta_B)^{-1}(\xi^{-1}\gamma\xi)(\xi^{-1}\phi_A, \bar{\eta}_A) = x_B^{-1}(\xi^{-1}\gamma\xi)x_A.$$

Thus the above tuples (x_A, x_B, γ) satisfy $x_B^{-1}(\xi^{-1}\gamma\xi)x_A \in \mu$. In this way, we have constructed a bijection

$$T \xrightarrow{\cong} \left\{(x_A, x_B, \gamma) \in [T(\mathbb{A}_f)/(T \cap K^\circ)]^2 \times B^\times \,\middle|\, x_B^{-1}(\xi^-1\gamma\xi)x_A \in \mu\right\}. \tag{7.3}$$

This is our desired overparametrization of $I(\mu)(\overline{\mathbb{F}}_p)$. We now want to get rid of the artificial pair (ϕ_A, ϕ_B). These form a simply transitive $T(\mathbb{Q})^2 = (L^\times)^2$-orbit where the action is

$$(y_A, y_B) \cdot (\phi_A, \phi_B) = (y_A \circ \phi_A, y_B \circ \phi_B).$$

In termis of the bijection (7.3), the action is described as

$$(y_A, y_B) \cdot (x_A, x_B, \gamma) = (y_A x_A, y_B x_B, y_B \gamma y_A^{-1}).$$

Assume that μ has regular semi-simple support and that (x_A, x_B, γ) is of relative position μ. Then γ does not normalize $L^\times \subset D^\times$ and hence

$$\mathrm{Stab}_{T(\mathbb{Q})\times T(\mathbb{Q})}(\gamma) = \{(z, z) | z \in \mathbb{Q}^\times\}.$$

Thus we may write

$$I(\mu)(\overline{\mathbb{F}}_p) = \bigsqcup_{\gamma \in L^\times \backslash D_{\mathrm{rs}}^\times / L^\times} \; \bigsqcup_{(x_A, x_B) \in T(\mathbb{A}_f)^2/\mathbb{Q}^\times} 1_\mu(x_B^{-1}\gamma x_A) \cdot (x_A, x_B, \gamma). \tag{7.4}$$

The next aim is to reinterpret (the counting of) this set as an orbital integral. This does not add new information, but it completes the journey: We have started from a group-theoretic situation (the Shimura data for GL_2 and T, the Hecke correspondence), have gone through all this formalism of algebraic geometry and moduli spaces, and then arrive back at a group-theoretic expression.

7.3. **Regular Semi-Simple elements II.** We briefly revisit the definition of regular semi-simple elements. Let k be a field, L/k a quadratic étale extension, D/k a quaternion algebra and $\rho : L \to D$ an embedding.

Example 7.4.
(1) $L = k \times k$ and $D = M_2(k)$. By Skolem–Noether (Thm. 7.1), we may assume ρ to be the inclusion of the diagonal matrices.
(2) $L/\mathbb{Q}$ an imaginary-quadratic field, $D/\mathbb{Q}$ the endomorphism ring of C as before and ρ the action of L on C.

The Galois conjugate embedding $\bar{\rho}$ is $D^\times$-conjugate to ρ by Skolem–Noether, i.e. there is $g \in D^\times$ with $g\rho(x) = \rho(\bar{x})g$ for all $x \in L$. This means that in the induced decomposition $D = D^+ \oplus D^-$ of D into L-linear and Galois-linear eigenspaces, both summands are free of rank 1 over L. We write $x = x^+ + x^-$ for the component decomposition of some $x \in D$.

In the following, we view $L^\times \times L^\times$ and $D^\times$ as algebraic groups. The former acts on the latter by the formula $(s, t) \cdot g = s^{-1}gt$.

Definition 7.5. An element $g \in D^\times$ is regular semi-simple if its stabilizer is of the minimal possible dimension and if its orbit is Zariski closed.

Proposition 7.6. *An element g is regular semi-simple if and only if $g^+, g^- \in D^\times$.*

Proof. All properties may be checked after extending scalars to $\bar{k}$, so we may assume that $L = k \times k$, that $D = M_2(k)$, and that ρ is the diagonal embedding. The component decomposition $g = g^+ + g^-$ is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & \\ & d \end{pmatrix} + \begin{pmatrix} & b \\ c & \end{pmatrix},$$

we need to see that g is regular semi-simple if and only if $abcd \neq 0$. If two entries vanish, then the stabilizer dimension is ≥ 2. Assume that precisely one entry vanishes, say c. We compute

$$\begin{pmatrix} s^{-1} & \\ & t^{-1} \end{pmatrix} \begin{pmatrix} a & b \\ & d \end{pmatrix} \begin{pmatrix} x & \\ & y \end{pmatrix} = \begin{pmatrix} s^{-1}ax & s^{-1}by \\ & t^{-1}dy \end{pmatrix}.$$

Take s any, t any, set $x = sa^{-1}$ and $y = td^{-1}$. This results in

$$\begin{pmatrix} 1 & s^{-1}btd^{-1} \\ & 1 \end{pmatrix},$$

showing that $\mathrm{diag}(1,1)$ lies in the closure of the orbit of g. The argument for other vanishing entries is analogous. In this way, we have proved that $abcd \neq 0$ is necessary for g to be regular semi-simple.

We now show sufficiency. The stabilizer of g is the set $((s,s),(s,s))$ and has dimension 1. Consider now the variety

$$U = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, abcd \in \mathbb{G}_m \right\} \subset \mathbb{A}^4$$

and the morphism

$$\mathrm{inv} : U \longrightarrow \mathbb{G}_m, \; g \mapsto a^{-1}bc^{-1}d.$$

We leave it as an exercise to see that $\mathrm{inv}(g_1) = \mathrm{inv}(g_2)$ if and only if they lie in the same orbit. (This holds S-points wise.) It follows that the orbit of some $g \in U(k)$ is $\mathrm{inv}^{-1}(\mathrm{inv}(g))$ and hence a closed subvariety. □

7.4. **Orbital Integrals.** We assume in the following that $K^\circ = \prod_{p<\infty} K_p$ decomposes as a product of open compact subgroups $K_p \subseteq G(\mathbb{Q}_p)$. We similarly assume $\mu^\circ = \prod_p \mu_p$.

Recall that on reasonable topological groups, there exists a (left-)translation invariant measure, called its Haar measure. It is unique up to scalar multiple. We normalize the Haar measure on $T(\mathbb{Q}_p)$ such that $\mathrm{Vol}(T \cap K_p) = 1$. We similarly take the Haar measure on $T(\mathbb{A}_f)$ with $\mathrm{Vol}(T \cap K) = 1$. Note that whenever one has an open $U \subseteq T(\mathbb{A}_f)$ that is a product $U = \prod_p U_p$, then $\mathrm{Vol}(U) = \prod_p \mathrm{Vol}(U_p)$.

Consider Haar measures on all $\mathbb{Q}_p^\times$ such that $\mathrm{Vol}(\mathbb{Z}_p^\times) = 1$ for almost all p. Then these define a product measure on the ideles $\mathbb{A}_f^\times$. For example, we could take the ones with $\mathrm{Vol}(\mathbb{Z}_p^\times) = 1$. In this case,

$$\mathrm{Vol}(\mathbb{Q}^\times \backslash \mathbb{A}_f^\times) = 1/2$$

because the class group of $\mathbb{Q}$ is trivial and $\mathbb{Z}^\times = \{\pm 1\}$. Here, we have applied an "obvious" definition of quotient measure: The quotient map $\pi : \mathbb{A}_f^\times \to \mathbb{Q}^\times \backslash \mathbb{A}_f^\times$ is a covering in the topological sense because $\mathbb{Q}^\times$ acts properly discontinuously. Given an open compact $U \subseteq \mathbb{A}_f^\times$ such that $\pi|_U$ is an isomorphism, $\mathrm{Vol}(\pi(U)) = \mathrm{Vol}(U)$.

This definition generalizes. Consider the quotient

$$\pi : T(\mathbb{A}_f)^2 \longrightarrow T(\mathbb{A}_f)^2 / \mathbb{A}_f^\times$$

where $\mathbb{A}_f^\times$ becomes a subgroup by $z \mapsto (z,z)$. Then there is a unique quotient measure that satisfies

$$\int_{T(\mathbb{A}_f)^2/\mathbb{A}_f^\times} \pi_*(f) = \int_{T(\mathbb{A}_f)^2} f \quad \text{for all } f \in C_c^\infty(T(\mathbb{A}_f)).$$

Here, $\pi_*(f)$ denotes the function obtained by integration over fibers. Very concretely, whenever one has an open compact $U \subseteq T(\mathbb{A}_f)^2$ such that $\mathrm{Vol}(\pi^{-1}(\pi(x))) = c$ is independent of $x \in U$ then

$$\mathrm{Vol}(\pi(K)) = \mathrm{Vol}(K)/c.$$

Similar considerations apply to all quotients $T(\mathbb{Q}_p)^2/\mathbb{Q}_p^\times$.

Definition 7.7. 1) For $f \in C_c^\infty(D(\mathbb{Q}_p)^\times)$ and $\gamma \in D(\mathbb{Q}_p)^\times_{\mathrm{rs}}$, define the orbital integral

$$O(\gamma, f) := \int_{T(\mathbb{Q}_p)^2/\mathbb{Q}_p^\times} f(h_1^{-1}\gamma h_2) dh_1\, dh_2.$$

2) For $f \in C_c^\infty(D(\mathbb{A}_f)^\times)$ and $\gamma \in D(\mathbb{A}_f)^\times_{\mathrm{rs}}$, define in the same way

$$O(\gamma, f) := \int_{T(\mathbb{A}_f)^2/\mathbb{A}_f^\times} f(h_1^{-1}\gamma h_2) dh_1\, dh_2.$$

The two orbital integrals are absolutely convergent because γ is assumed regular semi-simple. (The orbit $\{h_1^{-1}\gamma h_2\}$ being closed implies that its intersection with $\mathrm{Supp}(f)$ is still compact.)

Assume that $f_p \in C_c^\infty(D(\mathbb{Q}_p)^\times)$ is a family of test functions with the property that $f_p = 1_{\mathbb{Z}_p \otimes O_D}$ is the standard function for almost all p. Then the tensor product $f := \otimes_p f_p$, defined as

$$f\left((x_p)_p\right) := \prod_p f_p(x_p),$$

lies in $C_c^\infty(D(\mathbb{A}_f)^\times)$ and for every $\gamma = (\gamma_p)_p \in D(\mathbb{A}_f)^\times_{\mathrm{rs}}$ the adelic orbital integral factors as

$$O(\gamma, f) = \prod_p O(\gamma_p, f_p).$$

7.5. **Back to $I(\mu)$.**

Proposition 7.8. *The number of elements in $I(\mu)(\overline{\mathbb{F}}_p)$ is*

$$\mathrm{Vol}(\mathbb{Q}^\times \backslash \mathbb{A}_f^\times) \sum_{\gamma \in L^\times \backslash D^\times_{\mathrm{rs}}/L^\times} O(\gamma, 1_\mu).$$

Proof. This is now a reformulation of (7.4). □

8. CM Cycle Intersection III

The point count formula Prop. 7.8 was based on analyzing the set

$$\{(A, \eta, \rho : A \longrightarrow C) | (A, \eta) \in \mathcal{M}_K(\overline{\mathbb{F}}_p) \text{ and } \rho \text{ a quasi-isogeny}\}.$$

The purpose of today's lecture is to upgrade this from $\overline{\mathbb{F}}_p$-points to S-points; this is the idea underlying p-adic uniformization.

Let $\mathbb{F} := \overline{\mathbb{F}}_p$ and put $W = W(\mathbb{F})$. A scheme S over $\mathrm{Spf}\, W$ is the same as a scheme over $\mathrm{Spec}\, W$ such that $p \in \mathcal{O}_S$ is locally nilpotent. We denote by $\overline{S} := \mathbb{F} \otimes_W S$ the special fiber. For such S, we consider the set

$$\{(A, \eta, \rho : \overline{S} \times_S A \longrightarrow \overline{S} \times_{\mathrm{Spec}\, \mathbb{F}} C) | (A, \eta) \in M_K(S) \text{ and } \rho \text{ a quasi-isogeny}.$$

It is representable by a formal scheme, maps to M_K and allows to study its supersingular locus. The precise relation is given in Thm. 8.12 below.

In general, giving ρ is the same as giving a pair (ρ_p, ρ^p) of a p-quasi-isogeny ρ_p and an away-from-p quasi-isogeny ρ^p. The latter is a locally constant datum because $C[\ell]$ is étale for $\ell \neq p$. The datum ρ_p can vary non-trivially in families, which is described by the subgroup functors $\mathrm{Sub}_{p^m}(C[p^m])$ from last term. Thus for ρ_p, only the p^∞-torsion of C matters. For that reason, we pass to p-divisible groups. Another reason is that only this leads to a local definition of $\mathrm{Int}(g)$ as in Thm. 0.1.

8.1. **p-Divisible groups.** We work with schemes over $\operatorname{Spf}\mathbb{Z}_p$, i.e. S such that $p \in \mathcal{O}_S$ is locally nilpotent.

Definition 8.1. A p-divisible group of height h over S is an abelian fppf-sheaf X on S such that

(1) For every T/S and every $x \in X(T)$, there is some i with $p^i x = 0$.

(2) The multiplication map $[p] : X \to X$ is surjective.

(3) Each torsion subsheaf $X[p^i]$ is representable by a finite locally free S-group scheme of degree p^{hi}.

It follows that $X = \varinjlim_{i\geq 1} X[p^i]$, where the colimit is taken in fppf-sheaves. In fact, one often sees an equivalent definition just in terms of the inductive system

$$0 \longrightarrow X[p] \longrightarrow X[p^2] \longrightarrow \dots.$$

Theorem 8.2 ([8, Cor. II.3.3.16])**.** *Assume that $p^n\mathcal{O}_S = 0$ and let X/S be a p-divisible group. Then $\operatorname{Lie} X[p^n]$ is locally free over S and satisfies $\operatorname{Lie} X[p^n] = \operatorname{Lie} X[p^{n+k}]$ for all $k \geq 0$. It is denoted as $\operatorname{Lie}(X)$ and called the Lie algebra of X.*

Definition 8.3. We write $\operatorname{ht}(X)$ for the height of a p-divisible group. The (locally constant) integer $\dim(X) := \operatorname{rk}_{\mathcal{O}_S} \operatorname{Lie}(X)$ is called the dimension of X. In general $0 \leq \dim(X) \leq \operatorname{ht}(X)$.

Example 8.4. (1) Up to Galois twist, the only p-divisible group of height 1 and dimension 0 is constant group scheme $\mathbb{Q}_p/\mathbb{Z}_p$.

(2) Again up to Galois twist, the only one of height 1 and dimension 1 is the multiplicative group

$$\mu_{p^\infty} := \operatorname{colim}_{i\geq 0} \mu_{p^i} = \mathbb{G}_m[p^\infty].$$

(3) The main motivating examples are the p-divisible group of abelian varieties. Given A/S, define

$$A[p^\infty] := \varinjlim_{i\geq 1} A[p^i].$$

It is of dimension $\dim A$ and height $2\dim A$. Assume now that $S = \operatorname{Spec} k$ with $k = \bar{k}$ and that E/k is an elliptic curve. Then

$$E[p^\infty] = \begin{cases} \mathbb{Q}_p/\mathbb{Z}_p \times \mu_{p^\infty} & \text{if } E \text{ is ordinary} \\ \widehat{E} & \text{if } E \text{ is supersingular.} \end{cases}$$

The notation in the second case means formal completion along the identity. In both cases $E[p^\infty]$ is of dimension 1 and height 2, in the supersingular case however, we have no easy way of expressing the group law. The two occurring p-divisible groups are the unique ones over k of height 2 and dimension 1 (up to isomorphism).

(3) One could define p-divisible groups also in mixed characteristics. If $p \in \mathcal{O}_S^\times$ however, then all finite, locally free, p-torsion group schemes over S are étale, so every p-divisible group is just a Galois twist of $(\mathbb{Q}_p/\mathbb{Z}_p)^h$. The information of $A[p^\infty]$, for example, is then the same as that of $T_p(A)$. In particular, Thm. 8.2 fails in mixed characteristic and Def. 8.3 does not make sense anymore.

Given two p-divisible groups $X, Y/S$, one finds

$$\operatorname{Hom}(X, Y) = \varprojlim_{i\geq 0} \operatorname{Hom}(X[p^i], Y[p^i]),$$

which is a $\mathbb{Z}_p$-module. (A torsion-free one, in fact.) Just as with abelian varieties, a quasi-homomorphism is an element of

$$\mathrm{Hom}^0(X,Y) := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathrm{Hom}(X,Y),$$

while a (quasi-)isogeny is a (quasi-)homomorphism that is invertible as quasi-homomorphism.

We now state three important results on the relation of p-divisible groups with abelian varieties.

Proposition 8.5. *Let $A, B/S$ be abelian varieties. The following natural map is injective,*

$$\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathrm{Hom}(A,B) \longrightarrow \mathrm{Hom}(A[p^\infty], B[p^\infty]).$$

This is analogous to the classical statement about ℓ-adic Tate modules.

Proposition 8.6. *Let A/S be an abelian variety. There is a bijection*

$$\{p\text{-}(\textit{quasi-})\textit{isogenies } A \longrightarrow B\} \xrightarrow{1:1} \{(\textit{quasi-})\textit{isogenies } A[p^\infty] \longrightarrow Y\}.$$

Namely, giving a p-isogeny $A \to B$ up to isomorphism in B is the same as giving the kernel, which is contained in $A[p^\infty]$. This extends purely formally to quasi-isogenies.

Theorem 8.7 (Serre–Tate)**.** *Let $S_0 \hookrightarrow S$ be a nilpotent thickening and A_0/S_0 an abelian variety. Then*

$$\begin{aligned}&\{\textit{Deformations } (A, \gamma : S_0 \times_S A \cong A_0) \textit{ of } A_0 \textit{ to } S\}\\ \xrightarrow{1:1}&\{\textit{Deformations } (X, \gamma : S_0 \times_S X \cong A_0[p^\infty]) \textit{ of } A_0[p^\infty] \textit{ to } S\}.\end{aligned}$$

The following proposition shows that this bijection is compatible with endomorphisms.

Proposition 8.8. *Let $S_0 \to S$ be a nilpotent thickening, let $A, B/S$ be abelian varieties, put $A_0 = S_0 \times_S A$ and $B_0 = S_0 \times_S B$. A map $f_0 : A_0 \to B_0$ deforms to a map $f : A \to B$ if and only if $f_0|_{A_0[p^\infty]}$ deforms to a map $f' : A[p^\infty] \to B[p^\infty]$.*

Proof. By Grothendieck–Messing theory, Cor. 3.17 more precisely, some multiple $p^N f_0$ deforms to a map $(p^N f_0) : A \to B$. Then f_0 deforms if and only if $p^N f_0$ is divisible by p^N, which is equivalent to $A[p^N] \subseteq \ker(p^N f_0)$. This is equivalent to $p^N f_0|_{A[p^\infty]}$ being divisible by p^N, which is equivalent to f_0 deforming to $A[p^\infty]$. □

8.2. **Rapoport–Zink spaces.** We are now able to define RZ spaces; exciting!

Definition 8.9. Let $\mathbb{X}/\mathbb{F}$ be a p-divisible group. Consider the following functor on $\mathrm{Sch}/\operatorname{Spf} W$,

$$\mathcal{M}_{\mathbb{X}} : S \longmapsto \left\{ (X,\rho) \,\middle|\, \begin{array}{l} X/S \text{ a } p\text{-divisible group} \\ \rho : \overline{S} \times_S X \longrightarrow \overline{S} \times_{\overline{\mathbb{F}}_p} \mathbb{X} \text{ a quasi-isogeny} \end{array} \right\} / \cong$$

Two pairs (X,ρ) and (X',ρ') here are isomorphic if there is an isomorphism of p-divisible groups $\gamma : X \to X'$ such that $\rho = \rho' \circ \gamma$.

Theorem 8.10 (Rapoport–Zink [9, Thm. 2.16])**.** *The functor $\mathcal{M}_{\mathbb{X}}$ is representable by a formal scheme over* $\operatorname{Spf} W$ *that is locally formally of finite type and formally smooth of relative dimension* $\mathrm{ht}(X)(\dim(X) - \mathrm{ht}(X))$.

The idea of proof is as follows. First pick any deformation X_0 of $\mathbb{X}$ to W. Then one may also write

$$\mathcal{M}_{\mathbb{X}}(S) = \{(X, \rho) | \rho : S \times_W X_0 \longrightarrow X \text{ a quasi-isogeny}\}.$$

Now for each pair (d, N), one considers the locus in $\mathcal{M}_{\mathbb{X}}$ where ρ is of degree p^d and $p^N \rho$ an isogeny (no quasi here!). This is reperesentable by the subgroup functor from last term

$$\mathrm{Sub}_{p^{d+\mathrm{ht}(X)N}}(X_0[p^{d+\mathrm{ht}(X)N}]).$$

These subfunctors exhaust $\mathcal{M}_{\mathbb{X}}$ and the proof is about showing that they assemble to a formal scheme with the claimed properties.

8.3. **Example: The supersingular height 2 RZ space.** In previous chapters, we fixed a supersingular $C/\mathbb{F}$ and set $D = \mathrm{End}^0(C)$. Let $\mathbb{X} = C[p^\infty]$. Our aim is to describe $\mathcal{M}_{\mathbb{X}}$. First, as we have already seen,

$$\mathcal{M}_{\mathbb{X}}(\mathbb{F}) \xrightarrow{\cong} \mathbb{Z}, \quad (X, \rho) \longmapsto \log_p(\deg \rho).$$

The simple reason was that the only subgroups of $\mathbb{X} \cong \mathbb{F}[\![t]\!]$ are the $\mathrm{Spec}\, \mathbb{F}[t]/t^{p^d}$. Next, Thm. 8.7 implicitly states that the deformation functor of $\mathbb{X}$ is the same as that of C. Thus

$$\mathcal{M}_{\mathbb{X}} \xrightarrow{\cong} \coprod_{\mathbb{Z}} \mathrm{Spf}\, W[\![x]\!],$$

i.e. each connected component is isomorphic to $\mathrm{Spf}\, W[\![x]\!]$.

There are additional symmetries. We note without proof that the canonical map

$$\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathrm{End}(C) \longrightarrow \mathrm{End}(\mathbb{X})$$

is an isomorphism. In other words, $\mathrm{End}(\mathbb{X}) \cong O_{D_p}$ is a maximal order in a quaternion division algebra over $\mathbb{Q}_p$. In particular, $D_p^\times$ is the group of self-quasi-isogenies of $\mathbb{X}$. It acts on the RZ space by

$$D_p^\times \circlearrowright \mathcal{M}_{\mathbb{X}}, \quad \gamma \cdot (X, \rho) = (X, \gamma\rho).$$

Clearly

$$\log_p(\deg(\gamma\rho)) = \log_p(\deg \gamma) + \log_p(\deg \rho),$$

so this action is equivariant for the degree map $\mathcal{M}_{\mathbb{X}} \to \mathbb{Z}$. Recall that D_p is a valuation ring with normalized valuation

$$v : D_p^\times \longrightarrow \mathbb{Z}, \quad v(p) = 2.$$

Since $\deg(p) = p^2$ because $\mathbb{X}$ has height 2, we obtain

$$\log_p(\deg \gamma) = v(\gamma).$$

Write $\mathcal{M}_{\mathbb{X}}^d$ for the connected component of (X, ρ) with $\deg(\rho) = p^d$, let $\varpi \in D_p$ be a uniformizer. Then we see

$$\mathcal{M}_{\mathbb{X}}^0 \xrightarrow{\cong} \mathcal{M}_{\mathbb{X}}^d, \quad (X, \rho) \longmapsto (X, \varpi^d \rho).$$

We also obtain an action $O_{D,p}^\times \circlearrowright \mathcal{M}_{\mathbb{X}}^d$ for every connected component. This action is mysterious, however, I would not know of an explicit description in terms of coordinates.

8.4. **Uniformization.** Pick an additional full level structure $\xi : \mathbb{A}_f^2 \to V^p(C)$.

Lemma 8.11. *There is an isomorphism of functors on schemes $S/\operatorname{Spf} W$,*

$$\begin{aligned}&\{(A,\eta,\rho : \overline{S}\times_S A \longrightarrow \overline{S}\times_{\operatorname{Spec}\mathbb{F}} C)|(A,\eta)\in M_K(S) \text{ and } \rho \text{ a quasi-isogeny}\\ &\xrightarrow{\cong} GL_2(\mathbb{A}_f^p)^\times/K^{\circ,p}\times\mathcal{M}_{\mathbb{X}}\end{aligned} \tag{8.1}$$

by the assignment

$$(A,\eta,\rho)\longmapsto(\xi^{-1}\rho\eta,\rho[p^\infty]).$$

We leave this as a worthwhile exercise. Our next aim is to upgrade Prop. 6.5. Denote by $\widehat{M}_K^{\mathrm{ss}}$ the formal comletion of $W\otimes_{O_L} M_K$ along the closed subscheme $(W\otimes_{O_L} M_K)^{\mathrm{ss}}$ that consists of the finitely many supersingular points.

Theorem 8.12 (Uniformization of the supersingular locus)**.** *The forgetful map $(A,\eta,\rho)\mapsto(A,\eta)$ induces an isomorphism*

$$D^\times\backslash\left(GL_2(\mathbb{A}_f^p)/K^{\circ,p}\times\mathcal{M}_{\mathbb{X}}\right)\xrightarrow{\cong}\widehat{M}_K^{\mathrm{ss}}.$$

8.5. **Local intersection numbers.** Assume that p is inert in L so that $L_p/\mathbb{Q}_p$ is the unramified qudratic extension. We have fixed an action of L on C, providing us with an action of $O_{L,p}$ on $\mathbb{X}$. It satisfies the Kottwitz condition, i.e. the action on $\mathbb{X}$ is the natural one.

Definition 8.13. Denote by $\mathcal{C}\subseteq\mathcal{M}_{\mathbb{X}}$ the following closed formal subscheme. Its points $(X,\rho)\in\mathcal{C}(S)$ are those pairs with the property that

(1) $\rho O_{L,p}\rho^{-1}\subseteq\operatorname{End}(X)$, i.e. there is an $O_{L,p}$-action on X such that ρ is $O_{L,p}$-linear.

(2) This action satisfies the Kottwitz condition on $\operatorname{Lie}(X)$.

We explain (1). In general, $\rho O_{L,p}\rho^{-1}\subseteq\operatorname{End}^0(X)$ acts by quasi-homomorphisms. Thus given $x\in O_{L,p}$, we obtain an endomorphism of X as $p^N\rho x\rho^{-1}$ for $N\gg 0$. The condition of (1) (i.e. x lying in $\operatorname{End}(X)$) becomes $X[p^N]\subseteq\ker(p^N\rho x\rho^{-1})$. This is a closed condition, explaining why $\mathcal{C}$ is a closed formal subscheme.

Next, we describe $\mathcal{C}$. Again we first study $\mathcal{C}(\mathbb{F})$. Here, the degree function provides a bijection

$$\mathcal{C}(\mathbb{F})\longrightarrow 2\mathbb{Z},\quad (X,\rho)\longmapsto\log_p(\deg\rho).$$

The reason is, that any uniformizer $\varpi\in D_p$ satisfies $\varpi x=\bar{x}\varpi$ modulo $\varpi O_{D,p}$. Thus, even though (1) is satisfied for every point $(X,\rho)\in\mathcal{M}_{\mathbb{X}}(\mathbb{F})$, only half of the points satisfy the Kottwitz condition (2).

Grothendieck–Messing deformation theory, more precisely the canonical lifting Thm. 4.1, provides that $\mathcal{C}\to\operatorname{Spf} W$ is formally étale. It follows that

$$\mathcal{C}\xrightarrow{\cong}\coprod_{2\mathbb{Z}}\operatorname{Spf} W. \tag{8.2}$$

Given $\gamma\in D_p^\times$, we now consider the intersection

$$I(\gamma):=\mathcal{C}\cap\gamma\mathcal{C}.$$

Lemma 8.14. *Assume that $\gamma\in D_p^\times$ is regular semi-simple with respect to $L_p\subset D_p$. Then $I(\gamma)$ is a union of artinian schemes.*

Proof. We find $(X,\rho)\in\gamma\mathcal{C}$ if and only if $(X,\gamma^{-1}\rho)\in\mathcal{C}$. By definition, this implies that $\rho^{-1}\gamma O_{L,p}\gamma^{-1}\rho\subset\operatorname{End}(X)$. Since γ is regular semi-simple, $\gamma O_{L,p}\gamma^{-1}\neq O_{L,p}$, so $\dim_{\mathbb{Q}_p}\operatorname{End}^0(X)>2$. But the canonical lifting has endomorphism ring $O_{L,p}$. □

Just as with the orbital integral, there is a stabilizer here, namely the center $\mathbb{Q}_p^\times$ acts on $I(\gamma)$. The subgroup $p^{\mathbb{Z}}$ acts properly discontinuous because it shifts connected components by 2, the units $\mathbb{Z}_p^\times$ act trivially.

Definition 8.15. Define the intersection number

$$\begin{aligned}\mathrm{Int}(\gamma) &:= \ell_W(\mathcal{O}_{p^{\mathbb{Z}}\backslash I(\mu)}) \\ &= \ell_W(\mathcal{O}_{I(\mu)^0}),\end{aligned}$$

where $I(\mu)^0 \subset I(\mu)$ denotes the connected component where $\deg(\rho) = 1$.

Observe that $x\mathcal{C} = \mathcal{C}$ for every $x \in L_p^\times$. Thus $I(\gamma)$ and $\mathrm{Int}(\gamma)$ only depend on the orbit of γ in $L_p^\times \backslash D_p^\times / L_p^\times$. Recall that last time we defined an invariant

$$\mathrm{inv} : \mathbb{G}_m \times \mathbb{G}_m \backslash GL_{2,\mathrm{rs}} / \mathbb{G}_m \times \mathbb{G}_m \longrightarrow \mathbb{A}^1, \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto a^{-1}bc^{-1}d.$$

We are now dealing with $L_p^\times \backslash D_{p,\mathrm{rs}}^\times / L_p^\times$ instead and define an invariant in exactly the same way,

$$\mathrm{inv}(\gamma^+ + \gamma^-) = \mathrm{Nrd}_{D_p/\mathbb{Q}_p}((\gamma^+)^{-1}\gamma^-).$$

We leave it as an exercise to check that γ and γ' lie in the same orbit if and only if $\mathrm{inv}(\gamma) = \mathrm{inv}(\gamma')$. Assume $p \neq 2$ from now on. Concretely, $\mathrm{inv}(a + b\varpi) = pN_{L_p/\mathbb{Q}_p}(a^{-1}b)$ if ϖ is chosen as a uniformizer that normalizes L_p with $\varpi^2 = -p$.

Proposition 8.16. *If* $\mathrm{inv}(\gamma) \notin \mathbb{Z}_p$, *then* $\mathrm{Int}(\gamma) = 0$. *Otherwise,*

$$\mathrm{Int}(\gamma) = \frac{v_p(\mathrm{inv}(\gamma)) + 1}{2}.$$

Proof. The condition $\mathrm{inv}(\gamma) \notin \mathbb{Z}$ is equivalent to $v(b) < v(a)$, which is equivalent to $v(\gamma)$ being odd. In this case, $I(\gamma) = \emptyset$ because of the parity phenomenon in (8.2).

So let us assume $v(a) < v(b)$. For simplicity, we also impose $p \neq 2$. Multiplying by a^{-1}, we need to compute $I(1 + \gamma^-)^0$ with $\gamma^- \in O_{D,p}$. Write $O_{L,p} = \mathbb{Z}_p[\zeta]$ with $\bar{\zeta} = -\zeta$, pick a uniformizer ϖ with $\varpi\zeta = -\zeta\varpi$. Then we may write $\gamma = 1 + b\varpi$ with $b \in O_{L,p}$. We need to find the locus on $\mathcal{C}$ where

$$\gamma\zeta\gamma^{-1} = (1 + b\varpi)(1 - b\varpi)^{-1}\zeta$$

deforms to the quasi-canonical lifting. Since ζ acts as automorphism on the canonical lifting, this is equivalent to finding the locus to which

$$\frac{1 + b\varpi}{1 - b\varpi} \tag{8.3}$$

deforms. There exists a power series $\phi(x) \in \mathbb{Z}[\frac{1}{2}][\![x]\!]$ with

$$x = \phi\left(\frac{1+x}{1-x}\right),$$

so (8.3) deforms if and only if $b\varpi$ deforms. Now we apply the theorem of Gross (Thm. 4.3) to the canonical lifting $X/\mathcal{C}^0 \cong \mathrm{Spf}\, W$,

$$\mathrm{End}(W/p^n \otimes_W X) = O_{L,p} + p^{n-1}O_{D,p}.$$

Thus

$$I(\gamma)^0 = \mathrm{Spec}\, W/p^{v_p(b)+1}$$

and $v_p(b) + 1 = (v_p(\mathrm{inv}(\gamma)) + 1)/2$, finishing the proof. □

8.6. **Back to $I(\mu)$.** In the setting of §7.4, choose the local Haar measures on $\mathbb{Q}_p^\times$ such that $\mathrm{vol}(\mathbb{Z}_p^\times) = 1$. We have now seen all arguments for the following statement.

Theorem 8.17. *The length of the intersection $I(\mu)$ above p is given by*

$$\ell_{O_{L,p}}(\mathcal{O}_{I(\mu)_p}) = \mathrm{vol}(\mathbb{Q}^\times\backslash\mathbb{A}_f^\times) \sum_{\gamma\in L^\times\backslash D_{\mathrm{rs}}/L^\times} \mathrm{Int}(\gamma)O^p(\gamma, 1_{\mu^p}).$$

Here, $O^p(\gamma, 1_{\mu^p}) = \prod_{\ell\neq p} O_\ell(\gamma, 1_{\mu_\ell})$ is the product of orbital integrals over all primes $\neq p$.

References

[1] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, vol. 21, Springer Berlin & Heidelberg, 1990.

[2] A. Grothendieck, *Fondements de la géométrie algébrique. Extraits du Séminaire Bourbaki, 1957–1962.*, Secrétariat mathématique, Paris, 1962.

[3] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366.

[4] B. Fantechi, L. Göttsche, L. Illusie, S. L. Kleiman, N. Nitsure, and A. Vistoli, *Fundamental algebraic geometry. Grothendieck's FGA explained*, Mathematical Surveys and Monographs, vol. 123, American Mathematical Society, Providence, RI, 2005.

[5] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320.

[6] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162.

[7] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), no. 1-3, 437 – 449.

[8] W. Messing, *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes*, Lecture Notes in Mathematics, vol. 264, Springer-Verlag, Berlin-New York, 1972.

[9] M. Rapoport and T. Zink, *Period Spaces for p-divisible Groups*, Princeton University Press, 1996.

[10] The Stacks Project Authors, *Stacks Project*, Online, https://stacks.math.columbia.edu (2022).

[11] G. Cornell and J. H. Silverman (eds.), *Arithmetic Geometry*, Springer New York, 1986.

[12] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd Edition, Graduate Texts in Mathematics, vol. 106, Springer, 2009.